



Between Visibility and Vulnerability: Online Privacy Practices of Persons with Diverse Sexual Orientation and Gender Identities in Australia

Breanna Nobbs & Bhuva Narayan

To cite this article: Breanna Nobbs & Bhuva Narayan (28 Jun 2026): Between Visibility and Vulnerability: Online Privacy Practices of Persons with Diverse Sexual Orientation and Gender Identities in Australia, Journal of the Australian Library and Information Association, DOI: [10.1080/24750158.2026.2689217](https://doi.org/10.1080/24750158.2026.2689217)

To link to this article: <https://doi.org/10.1080/24750158.2026.2689217>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 28 Jun 2026.



[Submit your article to this journal](#)



Article views: 35



[View related articles](#)



[View Crossmark data](#)

RESEARCH

 OPEN ACCESS



Between Visibility and Vulnerability: Online Privacy Practices of Persons with Diverse Sexual Orientation and Gender Identities in Australia

Breanna Nobbs  and Bhuva Narayan 

School of Communication, University of Technology Sydney, Sydney, Australia

ABSTRACT

For persons with diverse sexual orientation and gender identities (SOGI), online spaces play a vital role in building community, finding information, exploring their identities and connecting with other individuals with diverse SOGI. These online interactions also help them in circumstances where an individual's daily life may not be a safe space to express themselves. This paper reports on an empirical study that explores the online privacy management practices of people with diverse SOGI in Australia, particularly as they relate to digital social media platforms that are global and often not based in Australia. In Australia, there is no constitutional right to privacy, and this can create challenges for vulnerable populations. Much of the discourse around privacy protection fails to consider precisely what role (if any) Australia's legal frameworks play in influencing the privacy management practices of persons with diverse SOGI. As online platforms are transnational and global, and as technology evolves quickly, the law inevitably cannot keep up. Because of this, social groups such as persons with diverse SOGI may be implicated and impacted by these developments in different ways.

ARTICLE HISTORY

Received 26 February 2026

Accepted 11 June 2026

KEYWORDS

Digital social media; information behaviours; privacy literacy; diverse sexual orientation and gender identities; SOGI; LGBTQIA+

A Note About the Terminology Used

We adopt diverse sexual orientation and gender identity or 'diverse SOGI' as a working term in this paper, while acknowledging that other initialisms exist. 'Diverse SOGI' aims to be more inclusive than other common terms as it includes people who choose not to identify under any of the existing initialisms, or whose identities are shifting. Terminology relating to persons with diverse SOGI has evolved rapidly, with researchers, academics, and government entities using a wide range of terms to describe people who do not conform to traditional gender and sexuality norms. 'Persons with diverse SOGI' intends to capture people with diverse sexual orientation and/or gender identities,

CONTACT Breanna Nobbs  Breanna.Nobbs@student.uts.edu.au  15, George Street, Ultimo, NSW 2007, Sydney, Australia

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

noting they may identify as one or both. The term diverse SOGI has been used by scholars (Daigle & Myrntinen, 2018; Mehra & Braquet, 2007) and international organisations such as the United Nations High Commissioner for Refugees (2015). Where we quote or draw directly from other works, we reproduce the authors' own terminology (e.g. LGBT, LGBTQ+, LGBTQIA+, queer), without alteration.

Introduction

How individual users of digital social media use online platforms differs across demographics, social groups, communities, and literacy levels, and varies among people with diverse sexual orientation and gender identity (SOGI). However, they may also face extra challenges around online privacy, especially due to any real or perceived tensions between their need for visibility and the vulnerability that comes with being open about their SOGI status.

In Australia, individuals are not protected by a single, comprehensive constitutional right to privacy as in some other countries. Instead, privacy protections come from a range of sources, such as statutory protections (for example, the Privacy Act 1988 (Cth) and State and Territory laws) and protections developed through the common law courts. Essentially, our rights are fragmented across various laws that can be eroded or removed in several ways, rather than being a fundamental constitutional right. Our right to privacy in international law is enshrined by the Universal Declaration on Human Rights (United Nations, 1948, art.12) (UNDHR) and the International Covenant on Civil and Political Rights (United Nations, 1966, art. 17) (ICCPR), among others, which are hard to enforce in the absence of domestic legislation, especially as the UNDHR is not a legally binding treaty and is a declaration, unlike the ICCPR.

It is worth noting that Australia is a party to the ICCPR and, through the Privacy Act, has 'undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy' (p. 1), partially fulfilling the ICCPR Article 17 obligations. In 2024, the Privacy Act underwent reforms and a statutory tort for serious invasions of privacy was introduced under the Privacy and Other Legislation Amendment Act 2024 (Cth) (POLA), which received Royal Assent on 10 December 2024, and commenced on 10 June 2025. Also introduced under the POLA, and effective from 11 December 2024, were changes to the Criminal Code Act 1995 (Cth) to make 'doxxing' a criminal offence. Doxxing is the act of maliciously releasing personal data, and under the new laws, aggravated doxxing includes offences against a group or member of a group because of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin. While it is important to address applicable domestic and international laws that frame this research more broadly, this paper does not explore which aspects of the frameworks or privacy provisions directly affect the participants.

As technology outpaces the legal framework, risks to people's privacy evolve alongside it, and the privacy protections that do exist may not adequately protect everyone equally. Legal and social frameworks may impact persons with diverse SOGI differently than those not part of this community.

This paper is based on a qualitative empirical study that explores how Australia's legal and regulatory framework relates to the online privacy management practices and

information behaviours of persons with diverse SOGI in Australia, especially as they relate to digital social media platforms, which are global and often not based in Australia. However, the focus of this paper is on how our participants manage their privacy online, especially information related to their SOGI identity, rather than a detailed exploration of Australian legal frameworks related to online privacy, except when participants themselves mention them.

Literature Review

This section reviews the various perspectives under which privacy is conceptualised and articulated, noting that it is a concept with no settled definition. Further, privacy and unique considerations for persons with diverse SOGI in the digital environment are explored, concluding with an overview of privacy literacy and information behaviour-related theories.

Concept of Privacy

According to Bawden and Robinson, privacy is ‘a complex and contested concept, whose very nature changes as information and communication technologies become more pervasive and omnipresent’ (2019, p. 2). Definitions of privacy are often derived from the works of legal scholars and commentators. For example, Westin, a professor of Public Law, defined privacy as ‘the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’ (1967, p. 7).

While legal scholars have actively contributed to the discussion of privacy, scholars from other faculties have also contributed. Nissenbaum observed that privacy, as proper flows of information within social contexts, remains a core challenge as technology rapidly evolves (2004). Nissenbaum’s work expands on Westin’s (1967) observations that, as individuals, we are ‘continually engaged in a personal adjustment process in which [we] balance the desire for privacy with the desire for disclosure and communication’ (p. 7). Solove (2002) defined privacy as a constructed phenomenon that is negotiated in social processes, consistent with Altman’s (1975) earlier view that privacy is ‘selective control of access to self or one’s group’. Solove (2006) expanded on their 2002 definition of privacy, creating a taxonomy of privacy threats that identifies four types of privacy harms arising from disclosing personal information (information collection, information processing, information dissemination, and invasion). This research relies on the *concept* of privacy rather than a single definition.

Privacy and the digital environment for persons with diverse SOGI

While the digital world exposes our private information to scrutiny from friends, family, strangers, and corporations, the risks of being ‘out’ are not universal and they remain ‘contextual and dependent on the person’ (Hanckel & Chandra, 2021, p. 20). Cho’s research found that for queer youth of colour, social media platforms such as Facebook embed a structural bias toward ‘default publicness’ through their design decisions, which assume that being out in public carries minimal risk (2018, p. 3185). Although people with

diverse SOGI use online platforms to construct and affirm their identity, managing this identity across multiple platforms involves careful calculation of each platform's audience expectations, social rules and risks (Colosi et al., 2023, pp. 6–8). The presence of unknown audiences complicates identity management, as discussed in Chen and Mares' research on social media self-presentation of LGBTQ+ youth, which found that 'sharing to mixed audiences leads LGBTQ+ youth to withhold or strategically manage their identity' (2025, p. 10). Johnson explored this phenomenon in their research and found that as platforms offer different experiences for users, LGBT*Q+ individuals were 'generally cautious' and would separate different social and family groups when using Facebook, so they do not intersect (2020, p. 90). This connects to the broader idea that social media allows for 'private exploration of SOGI in ways never before allowed' (Johnson, 2020, p. 9), but with this visibility comes a new risk of accidental outing online, through every post and privacy setting, and we ought to 'conceive coming out as a continual process' (p. 45). However, while online interactions and collective action can be important in forming a community, not all individuals within an online community will choose to share their personal information and experiences (Szulc & Dhoest, 2013).

These online interactions also serve as an important way to experiment with, explore and refine the outward expression of diverse SOGI identities, enabling individuals to test boundaries and cultivate an identity in ways that may not be available, are unsafe, or heavily constrained in their everyday offline lives (Bates et al., 2020; Duguay, 2016; Kuper & Mustanski, 2014). As noted above, this does not mean they share every intimate detail online; they may seek anonymity for certain things, and experiences will vary based on the individual and their unique circumstances. This is demonstrated by Hanckel et al.'s 2019 research, which drew on interviews with 23 LGBTIQ+ young people aged 16–35 across urban, regional and rural Australia, conducted in 2016 (p. 1266). Their research found that participants engaged in queer-world-building that 'circumnavigates platform policies and norms' to 'create collective moments of queer-world-building beyond the self' (pp. 1274–1275) in which a participant actively sought to be anonymous online to express what they could not express at home:

... I was basically anonymous so I could have whatever username I wanted, and I could just post. I would de-identify names and places and things, but I'd just post and re-blog stuff that I liked without having to filter ... Tumblr with [its] anonymous blog, helped me express when I couldn't express at home. (Jasmine, 26years, female, trans, trans-inclusive lesbian, urban) (p. 1274).

The idea of anonymity as a privacy management tool is further supported by Pingo & Narayan's 2019 study, which explored privacy management, knowledge of privacy frameworks and experiences with digital and social technologies. In this study, participants cited various reasons for not sharing personal information online, including security concerns and a desire to maintain boundaries between formal (e.g. work) and social relationships. While their study did not focus specifically on persons with diverse SOGI, it contextualises the overarching concepts of disclosure and boundary management as described in Petronio's (2002) Communication Privacy Management theory. When interacting online, these considerations are present in a person's decision-making, regardless of their SOGI status, but people with diverse SOGI are necessarily more aware of the implications.

While anonymity is one approach, it is essential to consider its limitations alongside the risks of disclosing personal information related to an individual's diverse SOGI status online. This is because 'social media platforms are unbounded spaces where messages cannot be contained and controlled, nor can they offer a uniform sense of engagement' (Byron, 2020, p. 81). Further, persons with diverse SOGI are at high risk of adverse implications to their private life, as they already 'experience disproportionately high rates of discrimination, marginalisation, harassment, abuse and violence' that, in the current online era, extends to digital communications (Powell et al., 2020, p. 206).

Privacy Literacy

Privacy literacy is the 'understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape' (Langenderfer & Miyazaki, 2009, p. 383) and is a concept that 'encompasses an informed concern for individuals' privacy and effective strategies to protect it' (Debatin, 2011, p. 51). Further, Park's (2013) views on online privacy literacy expand on this, describing it as a principle that supports, encourages, and empowers users to exercise informed control over their digital identities. Individuals may be considered privacy *literate* if they understand how the information they share will be stored, or used, and any risks involved with such disclosure. Conversely, individuals may be privacy *illiterate* if they disclose sensitive personal information with little understanding of the risks involved, including how their peers or strangers may use it to harm them and what the social networking site may do with it. Pingo and Narayan's (2019) research found that although participants engaged in active privacy management practices, this 'needed continual effort and continuous management on their part and hence was also a constant negotiation' (p. 47). They concluded that this 'privacy as negotiation' required 'an informed understanding of the fast-changing world of digital social media, which reiterates the role of privacy literacy' (p. 47).

Inaction around privacy has been described as the 'privacy paradox': individuals claim to care about their privacy, yet they behave in ways that do not reflect their concerns (Barnes, 2006; Kokolakis, 2017). This framing is contested by Draper and Turow (2019), who argue that it misrepresents resignation as ignorance or irrationality.

Information-Related Theories

This research is also informed by some Information Behaviour theories, specifically Information Overload and Anxiety (Bawden et al., 1999; Case, 2007), and Knowledge Gaps and Information Poverty (Chatman & Pendleton, 1995), which have been used to understand how individuals interact with information.

The concept of Knowledge Gaps and Information Poverty (Chatman & Pendleton, 1995) is grounded in the accessibility of information and in users' literacy to understand it. Case (2007) notes that 'when one human group (whether defined by income, education, location, or other variables) persistently differs from another human group in what they know, a knowledge gap is said to exist' (p. 101). Chatman and Pendleton discuss the concepts of first-level and second-level knowledge in response to the lack of consensus on the defining characteristics of a 'knowledge gap' and how to conceptualise information poverty. First-level knowledge is the knowledge of things that are

'known to us and to those with whom we share lived experiences with ... and are readily accessible, and sources have immediate verifiability' (1995, p. 143). Second-level knowledge, on the other hand, originates outside of our lived experiences, addressing things we have not experienced before, and 'verification of its truthfulness is problematic' (Chatman & Pendleton, 1995, p. 143).

Information overload is 'a state in which too much information leads to a generalised state of anxiety and/or confusion, or an inability to make a decision regarding a specific problem' (Case, 2007, p. 333). When too much information confronts us, we stop paying prompt and careful attention to some of it. This is also framed as 'information avoidance' by Case et al. (2005), who found that such avoidance can result from information overload, as well as from stress, anxiety, and a feeling of helplessness in the face of things one cannot control. This concept is much more individualistic, focusing on individuals' experiences and psychological and emotional responses, and complements the concept of knowledge gaps and information poverty.

Research Questions

Based on the literature above, the main research question and four sub-questions for this research are presented below. Focusing on the context of people with diverse SOGI using online digital social media, our main research question is:

What are the online privacy management practices of Persons with Diverse Sexual Orientations and Gender Identities? Specifically,

1. How do they *engage* with digital social media?
2. How do they *manage* their online identities?
3. What is their *awareness* of privacy laws?
4. What *impact* does digital social media have on the lives of persons with diverse SOGI?

Research Design

The methodological approach of digital ethnography was used to study the privacy management practices of persons with diverse SOGI, as it 'allows the researcher to examine the social interactions and information flow' and is the study of people in their online, real-world environment (Talip et al., 2017). Data was collected via an online survey (N = 150) and semi-structured interviews (including a digital walkthrough) of participants who self-selected to schedule and attend an interview at the end of the survey. 43 survey participants agreed to do interviews, and 15 interviews were completed in 2025. All institutional ethical clearance was obtained before data collection commenced (UTS Ethics ETH23-7883).

To assist in mitigating as many ethical concerns and risks as possible, a community advisory group (CAG) was formed with three community members who identify as people with diverse SOGI, and from a range of backgrounds: one Indigenous, one South Asian, and one Caucasian, all Australian citizens. The primary purpose of the CAG was to ensure ethical and inclusive research practices and to help identify any risks, weaknesses, and opportunities. CAGs are used across many disciplines, especially

in community-based health research and research with vulnerable groups. Indigenous research ethics also consider consultation groups or processes to be highly important, to ensure that research participants can make informed decisions and that the research process is honest and fair (George & Tauri, 2020).

Delimitations and Participant Selection

In addition to identifying as someone with diverse SOGI, participants were aged 18 or over, resided in Australia at the time of completing the survey or participating in an interview, and were regular social media users or at least comfortable navigating the internet. Participants who were irregular social media users were not excluded from our research, provided they were comfortable navigating the internet. This was because we aimed to capture a wide range of privacy management experiences, including factors that contribute to reduced online presence. Participants also had to understand English sufficiently and be comfortable participating in a semi-structured interview if selected.

This article does not discuss in detail Australia's legal privacy framework or its relationship to international legal privacy frameworks, as it is out of scope for this journal.

Online Survey

An online survey was used to gather high-level data from participants with diverse SOGI aged 18 and over residing in Australia. It was shared on various social media platforms (including Facebook groups the researchers belonged to, LinkedIn, and Instagram), via newsletters, and Microsoft Teams channels within our organisation. The survey contained structured questions, including open-ended, closed-ended, and multiple-choice questions, as well as questions on demographics, internet usage, and views on privacy and online privacy more generally. Additionally, much of the demographic information was free text or included a free-text option, allowing participants to self-identify or describe their identity, relationship status, and level of education. Age ranges of 18-25, 26-40, 41-55, and 55+ were provided to enable a wide range of participants.

The survey also served as a way for participants to self-select for a semi-structured interview. While the survey mainly served to recruit participants, responses to the open questions unrelated to demographics were analysed using Braun and Clarke's (2006) thematic analysis method and used to inform the semi-structured interview questions. These questions were finalised after reviewing survey responses to ensure that any themes, observations or concerns raised by participants were captured for further discussion during interviews. Simple statistical analysis was also used to analyse the survey results.

Semi-Structured Interviews and Digital Walkthrough Methodology

Semi-structured interviews were chosen to encourage a two-way, conversational dialogue, as they allow for more open-ended questions and flexibility (Williamson & Johanson, 2013). This format also allowed for participants' own voices to be represented in the

research (albeit anonymously) through their quotes when discussing findings (Bryman, 2016). In addition to semi-structured interviews, using the methodological approach of digital ethnography (Talip et al., 2016; Cavagnuolo et al., 2022), participants walked through their social media settings in their own online environment during the interview. The digital walkthrough helped to understand how participants actually interact with a digital interface rather than relying on what they remember about it.

The core of this method involves the step-by-step observation and documentation of an app's screens, features and flows of activity – slowing down the mundane actions and interactions that form part of normal app use in order to make them salient and therefore available for critical analysis (Light et al., 2018, p. 882).

Participants were asked to describe in detail the steps they took to complete specific tasks, rather than recounting what they think they have done or will do. This assisted in building an understanding of what influences participants' privacy management practices, and observations can be made on how their interview responses align with their practices. Compared to the semi-structured interview component, our digital walkthrough method used pre-defined questions to ensure consistency.

The 15 semi-structured interviews, including four pilot interviews, were part of the overall data analysis and were conducted online via Zoom and Microsoft Teams. Participants were given pseudonyms prior to commencing data analysis; the demographic spread of participants is in Table 1. Of the 15 participants who were interviewed, 14 agreed to participate in the optional digital walkthrough component. Interviews lasted between approximately 60–90 min, depending on each participant's responses and were recorded for transcription. Interviews were transcribed, hand-coded and analysed using Braun and Clarke's (2006) six-phase thematic analysis framework (initial coding, grouping of themes, reviewing themes, and defining themes). An inductive approach was taken, in which codes and themes were derived from the data rather than a deductive approach, which relies on established codes.

Of the participants interviewed, none identified as Aboriginal and Torres Strait Islander, and only three identified as culturally and linguistically diverse, including one participant who spoke another language at home.

Table 1. Information on interview participants.

No.	Participant ID	Age	Sexual orientation (SO)	Gender identity (GI)	Pronouns	State
1	A	18–25	Lesbian, Queer	Woman, Trans woman	She/Her	ACT
2	B	18–25	Lesbian	Woman, Trans woman	She/Her	ACT
3	C	26–40	Queer	Woman	She/Her	NSW
4	D	26–40	Bisexual	Trans woman	She/They	WA
5	E	26–40	Bisexual	Woman	She/Her	VIC
6	F	26–40	Pansexual	Non-binary	Any	ACT
7	G	26–40	Gay	Non-binary	He/They	QLD
8	H	18–25	Pansexual	Woman, Genderqueer/Genderfluid	They/She	NSW
9	I	26–40	Bisexual	Woman	She/Her	NSW
10	J	41–55	Gay	Man	He/Him	NSW
11	K	41–55	Gay	Man	He/Him	ACT
12	L	26–40	Pansexual	Woman	She/her	ACT
13	M	26–40	Gay	Man	He/Him	NSW
14	N	26–40	Bisexual	Woman	She/They	VIC
15	O	26–40	Lesbian	Woman	She/Her	SA

Research findings

The findings are presented here under the respective methods used for the data collection: the survey (N = 150), the semi-structured interviews (N = 15), and the digital walk-throughs (N = 14).

Findings from the Survey

As mentioned above, the survey was primarily used to establish eligibility to participate in the study and to elicit respondents' willingness to participate in the interviews. Of these, 43 expressed an interest in participating in one-on-one interviews, and a total of 15 in-depth interviews were conducted. We also included some open-ended questions in the survey, which are analysed here. Several key themes emerged from the perceptions and experiences of 150 respondents regarding social media and online privacy. A prominent theme is a pervasive concern about online privacy, data security and control, coupled with a significant lack of trust in corporations that run social media platforms. One participant noted:

I think I'm fairly cognisant of the data and privacy risks involved with using social media platforms, and I generally have low trust in corporations to not misuse my data. However, there's some dissonance there because, despite this, I do still use social media platforms.

Some respondents felt that privacy policies do not necessarily cover enough to protect user interests, while others noted they do not read privacy policies as they already presume any data or information given on the internet is no longer private. One respondent stated that:

Privacy terms and conditions can be really hard to navigate, and they don't remain static. While social media does provide an avenue to connect with diverse communities, I never feel truly safe and secure, as I feel every interaction is a data point that could be exploited or capitalised on by some entity.

This is similar to another respondent who raised the issue of feeling like they have no control over their information, yet they are still forced to use the platform to remain connected with family and friends. This theme also emerged during interviews, as discussed in the interviews section below.

Another theme that emerged from the open-ended survey responses was the affordances social media allows people with diverse SOGI to 'become different people online', noting it's 'a queer thing to have a few personas floating around'. This aligns with another respondent's views that 'online communities where I felt most anonymous was where I felt the most safe to start exploring LGBTQ content and interacting with others of similar dispositions'. However, some respondents expressed concerns about being outed to family and friends by being open about their identity on certain platforms, or through liking or interacting with content on platforms.

Findings from the Interviews

Throughout the 15 semi-structured interviews, several key themes emerged and are presented below in sections based on the thematic content analysis of the interview transcripts.

Identity, Community, and Support

Participants are simultaneously careful and strategic about sharing their SOGI identity. It can be a tool for visibility and creating safe spaces for many, but the decision to share is context-dependent, weighing factors like safety and the perceived openness of the audience. Most participants actively engage in risk assessments to determine what information to disclose. This risk assessment led Participant D to feel unsafe sharing information on public-facing platforms like TikTok and Twitter, specifically due to the common prevalence of ‘anti-queer, anti-trans [content]’. Participant G raised concerns about how people engage with social media, noting that:

Not many people engage with social media with social media literacy, and really kind of critically think about the content they’re consuming. They don’t use it in a safe way.

For those undergoing social or medical transitions, identity management is particularly fraught, and Participant A found that the ‘most confusing time’ for adjusting privacy settings was when she was in the process of changing her name socially. She had to carefully manage services to ensure that being known by ‘one name in one place’ didn’t accidentally reveal her previous identity if that service was linked to the wrong platform. This was after a negative experience where she accidentally interacted with someone’s post using her new identity before officially coming out as transgender, leading people to find out what she wasn’t yet ready to disclose at the time. However, online communities ultimately provided Participant A with the needed ‘safety for figuring out [her] identity’.

For Participant B, they decided to share their identity on their ‘Instagram close friends’ as a Story because ‘it’s somewhat ephemeral, but also it was sort of ... I wasn’t actively saying to anyone, it’s just sort of there if people saw it, which I felt more comfortable with’. This allowed Participant B to share their news without the ‘awkwardness’ of directly messaging people individually, especially those who were good friends in the past but maybe not in contact with now. However, for Participant I, her feelings about social media in general varied from platform to platform, but she described her online presence as:

I position myself as an observer. An observer of the world at large, but I do not engage with [social media], because the idea of being perceived by the public, and potentially, you know, misconstrued, misunderstood, or even just judged by the public, scares the hell out of me. It gives me a level of anxiety that I find really unmanageable.

When asked where they found the most joy or value in social media, Participant G described how social media helped find a community that he didn’t have access to offline:

Growing up queer in a small regional town, where I found joy in social media, was an online Lady Gaga fan website, because I could find queer community for the first time in a way that I just didn’t have access to in my offline worlds. Then, as I’ve gotten older and found more community, the joy has almost been social media as a way to organise and connect real life or in-person connection, and that’s been the joy to maintain a physical connection with people versus being the only form of connection.

Finding joy in both online and in-person interaction is also something Participant A experiences; however, she described maintaining connections as ‘so hard’ because we ‘have so much tech [and] life is just moving so quickly’. She also described her experiences with spending too much time online:

Sometimes, things in the real world and things in the online world are in two separate universes. It's sort of like ... it feels like they shouldn't really interact with each other. And specifically, sometimes, if I spend too much time on my phone, or just texting [with] people on the internet, then I sort of feel disconnected from the real world. And it sort of becomes a little bit scary sometimes.

Participant A also went on to say that she ultimately finds offline or 'real world' interaction to be a more 'fulfilling and rewarding experience' than interacting online, where she finds it more difficult to stay in touch with people.

Lack of Trust in Social Media Corporations versus the Compulsion to Use Social Media Platforms

Many participants expressed a clear lack of trust in social media corporations to protect users' data, often assuming their data is collected and sold, leading to feelings of resigned acceptance when using social media. Control efforts for most participants are focused on maintaining boundaries within known social circles, rather than confronting corporate data collection by the platforms or websites they use, which is perceived as beyond their control. Despite their privacy concerns, some participants find it difficult to leave platforms because they are the easiest way to stay connected to friends and family, or because they fear missing out on community or information. For example, Participant H noted that while they wanted to leave Meta platforms for ethical and political reasons, the primary factor stopping them was not wanting to 'lose contact' with friends living overseas. They stated:

The thing about it is that they have a monopoly over the social media landscape, so if you do want to leave, there [are] no real alternatives that can compete. So, it kind of creates this illusion of consent.

This is interesting, as Participant H also stated that it is common knowledge that 'our data is sold to make them money' and 'when you don't pay, you are the product'

Similarly, when asked if she has ever considered leaving these social media sites, Participant O described her efforts to leave the platforms and how she keeps coming back:

It's the easiest way to stay connected to my brothers. That is 100% the only reason I'm on there: it's the easiest way to see what [they] are doing. I don't like pushing myself into their lives.

Participant L, when asked how she felt about having to reinstall an application to maintain contact with one friend in the group, found it 'so annoying', stating 'I'm just missing this huge part of her life update, so I had to get it back'. Similarly, Participant E tried leaving Facebook but found it was 'too much of a hub' for contacting people, and Participant F discussed the difficulty of leaving group chats with friend groups and family groups, stating 'things that were established a long time ago ... it's hard to get your way out of'.

When questioned about the accessibility of social networking sites, Participant D discussed people who are more concerned with privacy than they are, leading them to boycott Meta applications and be concerned with TikTok. Participant D also discussed a 'real clear disbenefit' to not being on these platforms:

I think the fact that people are concerned about big tech companies and their attitudes towards privacy reduces the accessibility of those platforms, and because there's so much

that's organised on those platforms, there's so much that you're excluded from by not using them.

For Participant M, when he came out, he received many encouraging messages from friends and even strangers in response to sharing his experiences online. However, he also discussed trying to change his online identity as someone who:

works for LGBTQ advocacy, whose work is always revolving around the LGBTQ stuff. I really need to identify someone else as something else, you know, maybe a boring banker or a sheriff, something that has nothing to do with my sexuality. Because I don't feel like I want to be remembered as someone with only my LGBTQ stuff.

Addictive Nature of Social Media – Impact on Meaningful Connections

Several participants also discussed the addictive nature of social media applications, with Participant G stating that they use TikTok 'way too much, and it just sucks me in. Even when I'm frustrated and angry at it, it sucks me in, it's really terrible'. Participant K also described how 'tempting' it is 'to get drawn into the vortex and keep scrolling and scrolling and refreshing that Twitter feed'. Similarly, Participant A discussed their struggle with uninstalling one social media site, only for their behaviour to be replicated on another site:

So, my current situation with social media is that I uninstalled Instagram, like, over a year ago. It was, my main social media, and I uninstalled it because the reels were too addictive, and I just needed to go cold turkey. And it worked, which is great. Except it didn't really work, because now YouTube Shorts are very appealing.

When asked to describe what they like and dislike about social networking sites, Participant D noted that intentional community is only true of Instagram. However, this experience did not transfer to other sites they use:

Look, I do think they have their own culture, outside of just the specific people that

are ... your followers. I think Instagram is generally pretty positive. Twitter is very bitter, nasty and combative. TikTok, also full of randoms and unpredictable.

Participant K also described the generational use of some social media platforms and was of the view that Facebook is 'just not a platform for any sort of meaningful connection'. He also noted that:

What's interesting is, all my friends and I are obviously, even though I make a joke about my age, we are a Meta generation, so we all have the apps, but none of us use [Facebook] anymore ... we're not of the Snapchat generation. I mean, I have a Snapchat account, but I have no idea how to use it.

Professional and Personal Life Boundaries

For several participants, the fear of being judged by colleagues or of damaging their professional reputation influences what they share online, especially among those in careers where there is an expectation to maintain a certain public image. Most participants are cautious about adding colleagues on personal social media and often wait until someone leaves the workplace before connecting. However, Participant J described a considerable

shift in his view of privacy. He previously controlled who knew he was gay out of a 'fear of other people's judgement'. Whereas he now sees being openly gay on his public social media profiles as important to overcome that fear, demonstrating a shift away from concealing his identity.

When asked what she feels comfortable sharing (in general or in relation to her identity), Participant A described a constant battle when determining whether to disclose her identity:

Something that I've gone back and forth on for a while, is whether I want to be openly trans to lots of people. Because I kind of struggle with the two battles of ... I want people who maybe are less confident in themselves, or who feel like they're alone, to know that there are other trans people out there doing this sort of stuff, and who live mostly happy lives, etc. And on the other hand, I am aware of the safety aspect of people not knowing, because I think most people don't notice by looking at me, which is a privilege.

Interestingly, she made an active decision not to share her identity and was 'very conscious' about not telling people that she was trans during an internship, preferring to rely on her privilege of people not realising she is trans in the workplace.

Participant M discussed that the most 'feasible boundaries' he drew were separating 'work things and my personal life', citing a desire to only connect with colleagues on social media if there is a mutual enemy at work, otherwise, he chooses not to mix his work friends or colleagues with his personal life. Participant M further discussed having friends on Instagram that they feel know them enough to not 'question me about my sexualities or my obsessions [with] fashion or drag queens'. Interestingly he noted that he prefers new people don't know him from his account, rather 'they know me from myself, you know, from our interactions' stating he 'always play[s] with the feasibility and opacity of my level of privacy'.

While not specifically an online unwanted disclosure of his identity, when asked if he could recall an incident where he was shocked, surprised or offended by his private information being casually shared online by someone, Participant K recounted a time that he was outed in a gossip column before he told his parents he was gay. He felt 'quite violated' and recalls it was potentially shared in a digital version of the publication.

Location Sharing with Family and Friends

Many participants decide to share their location with friends, family or partners for a range of reasons such as security and convenience. Participant H always shares their location with their cousin, sister and parent for safety reasons. After their sister enabled it on each of their phones, they have 'left it on ever since'. Participant O also used location sharing with their wife to help reduce panic if they are home late from work. Participant K discussed the utility of location sharing, especially when visiting family or friends, where travel time may vary, stating they 'use it selectively on a sort of ad hoc and individual or closed group basis, and I guess that's a self-censoring privacy consideration there'.

Similarly, Participant M noted that in their home country, location sharing is essential because traffic is unpredictable and addresses are often imprecise.

Participant A originally used Life360 for safety reasons when moving to a new city; however, while starting her gender-affirming medical transition, she was 'terrified' that

her family would see her visiting the GP via location-sharing applications. This fear led her to temporarily stop sharing her location with them until she eventually came out and felt safe to reshare it. Some participants, such as Participant N, actively avoided location sharing even though they admitted it was useful at times. However, they wanted to have the freedom to say, ‘I’m busy, but be at home, or, you know, things like that ... just the privacy to not have your whereabouts shared all the time’. Similarly, Participant C stopped sharing with her partner because it eventually felt ‘unnecessary’.

Understanding of Privacy Laws and their Efficacy

Most participants had a general, often vague, understanding of Australian privacy laws, and many were quick to admit they do not know the specifics. However, a common sentiment was that Australian privacy laws are ‘pretty good’ compared to those in some other parts of the world. Many participants were familiar with privacy laws such as the General Data Protection Regulation (Article 9 of the Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119/1), with Participant A stating:

I know that the GDPR is a thing in the [European Union], and that it annoys website creators, and it’s the reason why you have to ... every time you go to a website, you have this big box that covers half the screen that says, “Do you want to accept the cookies?” And all I want is a big button that says, no, I don’t want to accept the cookies!

Participant C also spoke of her understanding that you had to select ‘allow cookies, because otherwise the website wouldn’t work properly’ and it wasn’t until watching an academic give a presentation that she ‘realised what was happening, and I was like, I don’t need to give away this stuff’.

Participants identified a tension between current privacy law frameworks and global digital platforms, expressing their doubt that existing laws meaningfully constrain corporate behaviour and data sharing. This tension led participants to rely on personal measures to protect their privacy instead. Participant A believes that because platforms are ‘so globalised’, Australian privacy laws likely have a ‘minimal impact’ in protecting our data and keeping people safe, stating they are ‘not relying on the privacy laws to keep my [information] private’. Participant D shared this sentiment, expressing awareness that social media sites are notorious for changing their policies and privacy protection, which ‘feels like something I have very little control over’. Participant E also shared this view and admitted to:

having no idea what the privacy laws actually entail, just the assumption they exist, and they probably ... I wouldn’t say they even stop data leaks. I would say they just mean that there are consequences if you get caught hacking or something like that. I don’t think it’s actively protecting, more just a consequence if you do something.

She was, however, familiar with her human right to not be discriminated against because of age, race, sexuality, gender, ‘and all those things’.

Findings from the Digital Walkthroughs

The digital walkthrough component of the interview process highlighted the consistent strategies participants used to address challenges related to digital privacy and identity

management. Participants generally agreed that finding and managing privacy controls at a granular level proved challenging and often required navigating through several unclear subheadings and/or pages.

Participants were asked to choose an application or platform they were familiar with and used frequently – chosen platforms included Facebook, Instagram, TikTok and X/Twitter. The initial step to access settings was consistent and intuitive, usually involving navigating to the profile and clicking the three horizontal lines (the ‘hamburger menu’) or an equivalent ‘Settings’ tab. Once past the initial menu, locating specific, deeper controls became difficult, and participants frequently had to use the search function because of the amount of information they needed to scroll through.

For some participants, features like Meta’s Account Centre caused confusion, adding a ‘whole separate step’ or making the hierarchy harder to grasp, especially when switching between Facebook and Instagram. The layout of settings was described as ‘hostile’ and ‘not easy’, leading to a feeling that options were deliberately ‘buried under layers of things I can’t figure out’. When faced with such confusion, the immediate reaction of many participants was to stop searching the application menus and instead ‘Google it’ for instructions.

Several participants grew frustrated with their chosen platform’s collection of personal data. Participants assumed platforms were collecting their data in exchange for access to the platform, but still desired clarity on exactly what was being collected. Privacy checks were often reactive, triggered by ‘other people’s mistakes and news stories’ (about data breaches) rather than proactive maintenance. Participants frequently concluded that, while the capacity for privacy control technically existed, platforms deliberately made it difficult, confirming a ‘tactic’ of a complex user experience to discourage setting management.

Discussion

This section connects the emergent findings with the literature and concludes with some answers to the research questions.

Engagement with Social Media

A common theme throughout the survey and semi-structured interviews was the desire to stay connected, with participants often maintaining social media accounts or downloading applications just to stay in touch with family and friends, creating an ‘illusion of consent’ in which they accept data practices they dislike, because no viable alternatives exist. This aligns with Nissenbaum’s (2004) observation that individuals must continually balance their desire for privacy with their desire for disclosure. For some participants, their social media engagement is often driven by a sense of social necessity and forced use, rather than pure choice. They were concerned about missing out on important information and connection, confirming Byron’s (2020) research, which found that most participants ‘did not enjoy the thought’ when asked to imagine their lives without social media (p. 40). This is complicated by what Cho (2018) identifies as the ‘default publicness’ of platform design, which assumes that being out in public carries minimal risk and does not account for the specific considerations of people with diverse SOGI.

Some participants noted deleting certain applications because they were sucked into a ‘vortex’ of infinite scrolling, even when they felt frustrated with the platforms. They also described feeling overwhelmed by the number of social media applications people are expected to use to stay up to date and in contact with friends and family, with in-person plans almost always made via social media.

Engagement varies by platform culture; for example, Instagram was viewed as a space for ‘intentional community’, while Twitter/X was seen as more combative, where one goes to find out who was wrong on the Internet today (Baughan et al., 2021; Paul, 2021). Participants rarely proactively used privacy checks, and they became salient only when triggered by news stories about data breaches or mistakes made by others. This connects with theories of information avoidance (2005), brought on by information overload, lack of time or too much cognitive load.

Online Privacy Management

Identity management for people with diverse SOGI is highly strategic and context-dependent. Some identity management tools include multiple personas, where participants leverage social media affordances to maintain multiple personas, using anonymity at times to safely explore content related to their diverse SOGI identity. This is a form of ‘queer world building’ that allows individuals to test boundaries and cultivate an identity that may be constrained in their everyday offline lives (Hanckel et al., 2019, pp. 1274–1275). Participant E noted that sharing personal stories and parts of her identity online is often intended for an ‘imagined audience’ (Litt, 2012) of everyone else in that community. It was surprising to hear a participant refer to the concept of an ‘imagined audience’, as described in the literature (Marwick & Boyd, 2011; Litt, 2012; Litt & Hargittai, 2016), indicating that it is common among those who post publicly.

Consistent with Petronio’s (2002) established Communication Privacy Management theory, whereby users create strict boundaries to separate formal (work) and social (personal) relationships, participants perform constant risk assessments to decide what to share, including using ‘close friends’ stories for ephemeral updates to avoid the ‘awkwardness’ of direct disclosure. This strategic visibility is also evident when maintaining professional boundaries. Participants described defaulting to locked-down profiles and choosing not to connect with colleagues on social media, doing so only after they left the workplace, demonstrating a strong emphasis on professional boundaries and strategic visibility.

Awareness of Privacy Laws

Most participants have a general, often vague, understanding of Australian privacy laws. However, most admit to not knowing specific details, including highly educated participants and lawyers, who demonstrated significant knowledge gaps regarding these frameworks. This illustrates ‘information poverty’ in which participants may have first-level knowledge of their daily experiences, but lack the second-hand knowledge required to verify the truthfulness of corporate data practices (Chatman & Pendleton, 1995).

Some participants are familiar with the GDPR, primarily through the ‘accept cookies’ boxes, though this was seen as annoying rather than a protective measure. There was also

a widespread belief that laws are reactive rather than proactive, only offering consequences after a privacy breach occurs, and that they have minimal impact on the behaviour of global corporations.

The digital walkthrough highlighted a persistent gap between the platforms' presentation of privacy policies and tools and participants' ability to effectively use them. This reinforces the notion that meaningful privacy control is often relegated to complex or hard-to-find sections of the social media application architecture, with participants often not feeling equipped or confident to navigate them. Privacy terms and conditions, as well as our regulatory and legal framework, seem to be evolving too quickly for participants to invest time to understand. One participant described Twitter/X's policies as 'circuitous', especially with respect to advertising. However, they still felt the platform gave them sufficient control, though the controls noted were mostly self-imposed, such as deciding what to post, rather than utilising the built-in tools.

Impact of Social Media

The intersection of diverse SOGI identity and digital privacy has several social and emotional consequences. There was a significant amount of distrust in institutions, with numerous participants assuming (and accepting) their personal information and data would be used for other purposes. This data collection and use led to a state of resigned acceptance, as described by Draper and Turow (2019), in which platform users assume their data is being sold anyway and feel they have no control over it. Participants also faced significant frustration with 'hostile' user interfaces that 'bury' privacy settings under layers of subheadings, which made meaningful privacy control feel inaccessible.

While online communities provide safety for figuring out identity, users live with the 'terrifying' possibility of being outed by platform features, such as location-sharing applications revealing visits to receive gender affirming healthcare. For some participants, the fear of being 'judged' or 'misunderstood' by a public audience causes unmanageable levels of anxiety, leading them to take on the role of an observer who does not actively post.

Conclusion

All users of digital social media are affected by privacy issues and disclosure online (Pingo & Narayan, 2019). However, for persons with diverse sexual and gender identities (SOGI), there are some unique and specific issues around their personal information and privacy that arise with their use of online digital social media, which not only affect their online lives, but also their everyday lives. Social media offers the allure of connection to many who are otherwise excluded from talking about their true selves, whether it be with family, friends, or in the workplace. Simultaneously, the threat of an identity breach by friends or cross-platform applications, or a privacy breach on platforms, is a continual issue, which some address by carefully curating multiple accounts, platforms, or even multiple identities. Others find it cognitively too hard to keep pace with every new development and either stop using certain platforms or choose to

ignore the issues for fear of losing their connections and networks, until a public privacy breach triggers them into action.

In general, there is significant room for improvement in privacy literacy, especially given the Australian regulatory framework in which we operate. Some participants felt they had sufficient control, however much of this was self-imposed rather than utilising platform features. Most participants were unable to find clear information about the personal data that platforms collect about them and how it is used.

While platforms such as Facebook have a 'common privacy settings' option to navigate through, digital social media platforms should have clear options to manage privacy, instead of common or big-ticket privacy controls being buried under layers of menus and subheadings. Users become overwhelmed when navigating through layers of options, and some give up entirely or resort to community answers.

Australia's privacy framework is slowly improving; however, the user community requires greater education and resources for privacy literacy, especially those from diverse SOGI or other minority groups, on how to safely interact online.

Acknowledgements

We would like to thank our survey participants and our interview participants, without whom this research would not have been possible.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

This research was supported by the Commonwealth through an Australian Government Research Training Program Scholarship [DOI: <https://doi.org/10.82133/C42F-K220>].

Notes on Contributors

Breanna Nobbs is a doctoral candidate at the School of Communication, Faculty of Design and Society at the University of Technology Sydney (UTS). She is a graduate of the ALIA-accredited Information and Media programme at UTS and a graduate of UTS: Law. She is currently a practising lawyer. Her research interests are in human information behaviours, big data, digital social media, privacy law, and international law. The views expressed in this article are solely those of the author and do not reflect the views or policies of the author's employer.

Bhuva Narayan is Associate Professor in the School of Communication, Faculty of Design and Society at the University of Technology Sydney (UTS). Bhuva was Head of Discipline for the Information and Knowledge Management Courses, an ALIA-accredited Library and Information Science programme at UTS from 2013 to 2018, and Director of the Graduate Research Programme at the Faculty of Arts and Social Sciences from 2019 to 2024 and the Director of the Graduate Research Programme at the new Faculty of Design and Society at UTS from 2025-2026. Her research areas are in library and information science, specifically information behaviours, information avoidance, information access, user experience, human learning, human-computer interaction, personal information management, documentation studies, scholarly communication and open access. She is associate editor of the Journal of the Australian Library and Information Association (JALIA).

ORCID

Breanna Nobbs  <http://orcid.org/0009-0003-1137-979X>

Bhuva Narayan  <http://orcid.org/0000-0001-8852-5589>

References

- Altman, I. (1975). *The environment and social behavior: Privacy, personal space territory, and crowding*. Brooks/Cole Publishing Company.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9), <https://doi.org/10.5210/fm.v11i9.1394>
- Bates, L., Hobman, T., & Bell, B. T. (2020). "Let Me Do What I Please With It ... Don't Decide My Identity For Me": LGBTQ+ youth experiences of social media in narrative identity development. *Journal of Adolescent Research*, 35(1), 51–83. doi:[10.1177/0743558419884700](https://doi.org/10.1177/0743558419884700)
- Baughan, A., Petelka, J., Yoo, C. J., Lo, J., Wang, S., Paramasivam, A., Zhou, A., & Hiniker, A. (2021). Someone is wrong on the internet: Having hard conversations in online spaces. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1–22. doi:[10.1145/3449230](https://doi.org/10.1145/3449230)
- Bawden, D., Holtham, C., & Courtney, N. (1999). Perspectives on Information Overload. *Aslib Proceedings*, 51(8), 249–255. <https://doi.org/10.1108/EUM0000000006984>
- Bawden, D., & Robinson, L. (2019). Essentially made of information": Concepts and implications of informational privacy. *Information Research*, 24(4), Colis1913. <http://InformationR.net/ir/24-4/colis/colis1913.html>.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. doi:[10.1191/1478088706qp0630a](https://doi.org/10.1191/1478088706qp0630a)
- Bryman, A. (2016). *Social research methods*. Oxford University Press.
- Byron, P. (2020). *Digital media, friendship and cultures of care*. Taylor & Francis Group.
- Case, D. O. (2007). *Looking for information*. Emerald Publishing Limited.
- Case, D. O., Andrews, J. E., Johnson, J. D., & Allard, S. L. (2005). Avoiding versus seeking: the relationship of information seeking to avoidance, blunting, coping, dissonance, and related concepts. *Journal of the Medical Library Association*, 93(3), 353.
- Cavagnuolo, M., Capozza, V., & Matrella, A. (2022). The walkthrough method: State of the art, innovative aspects, and application fields. In G. Punziano, & A. Delli Paoli (Eds.), *Handbook of research on advanced research methodologies for a digital society* (pp. 461–486). IGI Global Scientific Publishing.
- Chatman, E. A., & Pendleton, V. E. (1995). Knowledge gap, information-seeking and the poor. *The Reference Librarian*, 23(49-50), 135–145. doi:[10.1300/J120v23n49_10](https://doi.org/10.1300/J120v23n49_10)
- Chen, Y. A., & Mares, M. L. (2025). Social media self-presentation of LGBTQ+ youth in the United States: The role of identity exploration, context collapse, and supportive feedback. *Journal of Computer-Mediated Communication*, 30(6), zmaf020. <https://doi.org/10.1093/jcmc/zmaf020>
- Cho, A. (2018). Default publicness: Queer youth of color, social media, and being outed by the machine. *New Media & Society*, 20(9), 3183–3200. <https://doi.org/10.1177/1461444817744784>
- Colosi, R., Cowen, N., & Todd, M. (2023). Sexual and gender identity work on social media. *Sociology Compass*, 17(6), e13073. <https://doi.org/10.1111/soc4.13073>
- Criminal Code Act 1955 (Cth). <https://www.legislation.gov.au/C2004A04868/2018-12-29/text>.
- Daigle, M., & Myrntinen, H. (2018). Bringing diverse sexual orientation and gender identity (SOGI) into peacebuilding policy and practice. *Gender & Development*, 26(1), 103–120. doi:[10.1080/13552074.2018.1429091](https://doi.org/10.1080/13552074.2018.1429091)
- Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 47–60). Springer.
- Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 1824–1839. doi:[10.1177/1461444819833331](https://doi.org/10.1177/1461444819833331)
- Duguay, S. (2016). He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society*, 18(6), 891–907. <https://doi.org/10.1177/1461444814549930>

- George, L., & Tauri, J. (2020). *Indigenous research ethics: Claiming research sovereignty beyond deficit and the colonial legacy*. Emerald Publishing.
- Hanckel, B., & Chandra, S. (2021). *Social media insights from sexuality and gender diverse young people during COVID-19*. Western Sydney University.
- Hanckel, B., Vivienne, S., Byron, P., Robards, B., & Churchill, B. (2019). 'That's not necessarily for them': LGBTIQ plus young people, social media platform affordances and identity curation. *Media, Culture & Society*, 41(8), 1261–1278. <https://doi.org/10.1177/0163443719846612>
- Johnson, P. M. (2020). *Coming out queer online: Identity, affect, and the digital closet*. Bloomsbury Publishing PLC.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. doi:10.1016/j.cose.2015.07.002
- Kuper, L., & Mustanski, B. S. (2014). Using narrative analysis to identify patterns of Internet influence on the identity development of same-sex attracted youth. *Journal of Adolescent Research*, 29(4), 499–532. <https://doi.org/10.1177/0743558414528975>
- Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *Journal of Consumer Affairs*, 43(3), 380–388. doi:10.1111/j.1745-6606.2009.01152.x
- Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, 20(3), 881–900. doi:10.1177/1461444816675438
- Litt, E. (2012). Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media*, 56(3), 330–345. <https://doi.org/10.1080/08838151.2012.705195>
- Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media + Society*, 2(1), 2056305116633482. <https://doi.org/10.1177/2056305116633482>
- Marwick, A. E., & Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133. doi:10.1177/1461444810365313
- Mehra, B., & Braquet, D. (2007). Library and information science professionals as community action researchers in an academic setting: Top ten directions to further institutional change for people of diverse sexual orientations and gender identities. *Library Trends*, 56(2), 542–565. doi:10.1353/lib.2008.0005
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119.
- Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215–236. <https://doi.org/10.1177/0093650211418338>
- Paul, J. (2021). Someone is wrong on the internet: Is there an obligation to correct false and oppressive speech on social media? In A. MacKenzie, J. Rose, & I. Bhatt (Eds.), *The epistemology of deceit in a postdigital era* (Postdigital Science and Education) (pp. 1–10). Springer. https://doi.org/10.1007/978-3-030-72154-1_8
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.
- Pingo, Z., & Narayan, B. (2019). Privacy literacy and the everyday use of social technologies. In S. Kurbanoğlu, S. Špiranec, Y. Ünal, J. Boustany, M. L. Huotari, E. Grassian, D. Mizrachi, & L. Roy (Eds.), *Information literacy in everyday life* (Communications in Computer and Information Science, Vol. 989, pp. 33–49). Springer. https://doi.org/10.1007/978-3-030-13472-3_4
- Powell, A., Scott, A. J., & Henry, N. (2020). Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology*, 17(2), 199–223. <https://doi.org/10.1177/1477370818788006>
- Privacy Act 1988 (Cth). <https://www.legislation.gov.au/C2004A03712/latest/text>.
- Privacy and Other Legislation Amendment Act 2024 (Cth). <https://www.legislation.gov.au/C2024A00128/asmade/text>.
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90(4), 1087. doi:10.2307/3481326
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. <https://doi.org/10.2307/40041279>
- Szulc, Ł., & Dhoest, A. (2013). The internet and sexual identity formation: Comparing Internet use before and after coming out. *Communications*, 38(4), 347–365. <https://doi.org/10.1515/commun-2013-0021>

- Talip, B. A., Narayan, B., Edwards, S. L., & Watson, J. (2017). Digital ethnography as a way to explore information grounds on Twitter. *Qualitative and Quantitative Methods in Libraries*, 5(1), 89-105.
- United Nations. (1966). International covenant on civil and political rights. *United Nations Treaty Series*, 999, 171. <https://www.ohchr.org/en/instrumentsmechanisms/instruments/international-covenant-civil-and-political-rights>.
- United Nations General Assembly. (1948). *Universal Declaration of Human Rights (Resolution 217A)*. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- United Nations High Commissioner for Refugees. (2015). *Protecting persons with diverse sexual orientations and gender identities: A Global Report on UNHCR's Efforts to Protect Lesbian, Gay, Bisexual, Transgender, and Intersex Asylum-Seekers and Refugees*. <https://www.unhcr.org/en-au/publications/brochures/5ebe6b8d4/protectingpersons-diverse-sexual-orientation-gender-identities.html>.
- Westin, A. (1967). *Privacy and freedom*. Atheneum Press.
- Williamson, K., & Johanson, G. (Eds.). (2017). *Research methods: Information, systems, and contexts*. Chandos Publishing.