

# From Phreaking to Sneaking: Children’s Circumvention of Social Media Age Verification Systems

Bjørn Nansen ↗

School of Computing and Information Systems, The University of Melbourne  
nansenb@unimelb.edu.au

Helena Sandberg ↗

Department of Communication, Lund University, Sweden  
Helena.Sandberg@iko.lu.se

Lauren Bliss ↗

School of Computing and Information Systems, The University of Melbourne  
Lauren.bliss@unimelb.edu.au

Shaanan Cohney ↗

School of Computing and Information Systems, The University of Melbourne  
shaanan@cohney.info

---

## Abstract

Australia’s social media ban is now in force. It requires platforms to take reasonable steps to stop users under 16 from holding accounts. Drawing on five focus groups with fifteen young people aged 12–16, this paper examines how children understood the ban’s effectiveness, impact, and legitimacy as they encountered the platforms charged with enforcing it. Participants widely saw the ban as unfair and ineffective. Through platform access controls, they learned how the ban worked, where it failed, and how they and their peers could evade it. We also asked participants to imagine better approaches to age verification and youth digital governance.

This paper develops *sneaking* as a theoretical lens for these practices. The concept names more than evasion: it captures the social encounter between children, platforms, techno-regulation, and the access controls that mediate digital participation. Our findings show that children are not passive subjects of platform regulation. They interpret, test, and negotiate digital infrastructure. They also expose a central weakness in age-based platform regulation: technological controls struggle to solve the social and governance problems they are asked to contain.

---

All authors were equally and collaboratively involved in all aspects of the research paper, including conception and design, data collection and analysis, drafting and revision, critical input, and approval of the final submitted version; all authors agree to be accountable for all aspects of the work.

# 1 Introduction

In late 2025, Australia became the first country to ban social media for users under 16. This paper examines how children directly affected by the ban responded. Drawing on focus groups with children aged 12–16, we ask how they viewed, navigated and, in many cases, circumvented, the technologies implementing Australia’s social media restrictions. Our participants broadly disagreed with the ban; and frequently bypassed it. The participants described both uneven platform enforcement and their tactics and rationales for keeping access to social media. To theorise these practices, we develop the concept of social network *sneaking* – a concept which draws on the technical and cultural legacy of phreaking. We use this framing to analyse children’s development of a culture of bypassing age verification systems, while also suggesting its broader relevance for understanding how users work around digital restrictions generally. This lens also emphasises children’s rights in digital environments (Livingstone and O’Neill 2014; UN Committee on the Rights of the Child 2021)<sup>1,2</sup>, especially their rights to information provision, participation, and protection.

We identify four themes that capture our participants’ approach to sneaking: 1) young users learn through experimentation how age verification systems work; 2) they manipulate systems to bypass restrictions; 3) they share vernacular knowledge about vulnerabilities; 4) and they imagine and attempt to contribute to alternative futures. Across these themes, children’s circumvention appears less as an overt challenge to authority than as a pragmatic negotiation with digital infrastructure – much like the early culture of “hackers”. This connects sneaking to concerns in studies of infrastructure politics about platform governance and the limits of technical enforcement, which we return to in the discussion. Young people’s response to existing systems is more than passive. Children’s everyday workarounds represent an emerging engagement with the politics of digital infrastructure, which we argue that this demonstrates their capacity to imagine fairer forms of digital governance. In our framework, young users are not merely subjects of control but rights-bearing agents who interpret, navigate, and work around systems they perceive as unjust or misaligned with their lives.

## 2 Background and Context

### 2.1 The Australian Age Restrictions and Age Verification Technologies

Australia’s recent restrictions on children’s access to social media platforms are a world-first: no prior law had imposed on platforms a *positive obligation to take reasonable steps*, typically through age assurance measures, to prevent under-16s from holding accounts (Champion et al. 2025; eSafety Commissioner 2026a; Online Safety Amendment (Social Media Minimum Age) Act 2024)<sup>3,4,5</sup>. The restrictions took effect on December 10, 2025 (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts 2025b)<sup>6</sup>.

Children’s own experiences of the ban are an especially important and thus far understudied phe-

---

<sup>1</sup> S. Livingstone and B. O’Neill (2014). *Children’s rights online: Challenges, dilemmas and emerging directions*. In S van der Hof, B van den Berg, B Schermer (Eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Springer, 19-38.

<sup>2</sup> UN Committee on the Rights of the Child (2021). *General comment No. 25 (2021) on children’s rights in relation to the digital environment*.

<sup>3</sup> K. E. Champion et al. (2025). *Debate: Social media in children and young people—time for a ban? Beyond the ban—empowering parents and schools to keep adolescents safe on social media*. *Child and Adolescent Mental Health*, 30(4): 411-413.

<sup>4</sup> eSafety Commissioner (2026a). *Social Media Age Restrictions*.

<sup>5</sup> Online Safety Amendment (Social Media Minimum Age) Act (2024). (Cth).

<sup>6</sup> Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2025b). *Social Media Minimum Age*.

nomenon. Although extensive research examines children’s online safety and media use (e.g., Gath and Swit 2024; Smahel et al. 2020; Stoilova et al. 2021)<sup>7,8,9</sup>, much less empirical work has examined how young people encounter age verification technologies or how abrupt policy shifts reshape their access to, and practices around, social media. This matters beyond Australia because the ban is already being explicitly cited in active policy and legislative processes elsewhere, including a UK government consultation on minimum age for social media access, a French parliamentary bill to ban social media for under-15s, and German proposals for age-based social media curbs (Department for Science, Innovation and Technology 2026; Reuters 2026a; Reuters 2026b)<sup>10,11,12</sup>. Through youth-centred qualitative methods, this paper shows how regulation, platform infrastructure, and children’s agency interact, and contributes to debates about the ethical design of verification systems and youth protection policy in digital environments.

In practice, compliance is relying on a range of age assurance mechanisms, including document-based checks (credit cards/IDs), machine-learning systems that estimate age from a photo or video of a user’s face, and systems that infer a users’ age based their platform use. Among these, facial age estimation systems have attracted particular public attention. Unlike document-based checks, these systems are designed to estimate whether a user falls within a given age range rather than verify their identity. This reduces reliance on government-issued identification, but introduces a different set of technical and normative concerns. State-of-the-art facial age-estimation systems still produce non-trivial false-positive and false-negative errors, especially in age bands close to relevant policy thresholds. Further NIST evaluations of face-analysis systems have also documented demographic performance differentials, including skin-tone-related effects in some error patterns (Hanaoka et al. 2024; Grother et al. 2022)<sup>13,14</sup>. The models also raise distinct privacy concerns (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts 2025a; HF and An Nur 2025; Köhler-Dauner et al. 2025; Lueks et al. 2026)<sup>15,16,17,18</sup>.

The policy is controversial not only because of the technologies on which it may depend, but also because of Australia’s policy design and implementation. Critics point to uneven platform coverage, the chosen age threshold, rushed passage of the law, gaps in the robustness of implementations, and unintended consequences for both child and adult users (eSafety Commissioner 2026a; Taylor 2026; Rubinstein et al. 2024)<sup>19,20,21</sup>. These implementation concerns also expose a deeper policy tension:

---

<sup>7</sup> M. Gath and C. Swit (2024). *Digital media in early childhood: Risk factors for online harm and psychosocial correlates*. *Frontiers in Developmental Psychology*, 2, Article 1390276.

<sup>8</sup> D. Smahel et al. (2020). *EU Kids Online 2020: Survey Results From 19 Countries*. *EU Kids Online*.

<sup>9</sup> M. Stoilova et al. (2021). *Children’s understanding of personal data and privacy online: A systematic evidence mapping*. *Information, Communication & Society*, 24(4): 557-575.

<sup>10</sup> Department for Science, Innovation and Technology (2026). *Growing Up in the Online World: A National Consultation*. GOV.UK.

<sup>11</sup> Reuters (2026a). *French Senate debates social media ban for children under 15*. Reuters.

<sup>12</sup> Reuters (2026b). *Germany’s ruling party backs social media curbs for children*. Reuters.

<sup>13</sup> K. Hanaoka et al. (2024). *Face Analysis Technology Evaluation: Age Estimation and Verification*. *National Institute of Standards and Technology*, NIST IR 8525.

<sup>14</sup> P. Grother et al. (2022). *Face Recognition Vendor Test (FRVT): Demographic Summaries*. *National Institute of Standards and Technology*, NIST IR 8429.

<sup>15</sup> Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2025a). *Age Assurance Technology Trial: Final Report*.

<sup>16</sup> N. H. HF and F. An Nur (2025). *Constructing childhood realities: A communication science analysis of TikTok’s age verification failure and psychosocial impact*. *Legal Brief*, 14(3).

<sup>17</sup> F. Köhler-Dauner et al. (2025). *Digital child protection in social networks: Age verification and age-tiered regulation in Europe* *Child and Adolescent Psychiatry and Mental Health*, 19, Article 143.

<sup>18</sup> W. Lueks et al. (2026). *Assessing age assurance technologies: Effectiveness, side-effects, and acceptance*. *arXiv*.

<sup>19</sup> eSafety Commissioner, *supra* note 4.

<sup>20</sup> J. Taylor (2026). *Australia wants to sell its social media ban to the world – but are the measures even working?* *The Guardian*, April 1.

<sup>21</sup> B. I. P. Rubinstein et al. (2024). *Submission 272 to the Senate Environment and Communications Legislation Committee: Online Safety Amendment (Social Media Minimum Age) Bill 2024*.

how to protect children while respecting their developing autonomy and right to inclusion in digital life (Stalford and Lundy 2025)<sup>22</sup>. Children’s involvement in decisions about digital policies matter because their everyday social, educational, and civic practices are now deeply embedded in digital environments (Köhler-Dauner et al. 2025; Livingstone and Third 2017)<sup>23,24</sup>.

Whether these measures are justified depends in part on whether they can deliver their stated benefits in practice. Before implementation, public reporting had already identified VPNs, AI-generated images, and disguise-based attempts as likely bypass vectors (Lavoipierre 2025)<sup>25</sup>. Yet eSafety’s March 2026 compliance update and subsequent reporting (Butler 2026)<sup>26</sup> indicated that many children retained or regained accounts. Similarly, eSafety’s own survey of parent’s suggested that around seven in ten children with accounts on several major platforms still had access (eSafety Commissioner 2026b; Taylor 2026)<sup>27,28</sup>. This is consistent with our findings. Our young participants described age verification as easy to circumvent. These accounts sit uneasily alongside a government-commissioned report, prepared by an industry partner from the age assurance industry, which claimed that age assurance could be implemented privately, efficiently, and effectively (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts 2025a)<sup>29</sup>.

Drawing on youth-centred qualitative methods this paper offers an original account of the interplay between regulation, platform infrastructure, and children’s agency. This contributes directly to the ethical design and implementation of emerging verification systems and the refinement of youth digital protection policies. The discussion suggests that children may not simply encounter the ban as a rule to obey or resist. Rather, the interaction is an encounter with a technical system to be interpreted, tested, and worked around. In the following subsection, we develop a lens to enrich our discussion of the interaction’s collective, knowledge-sharing, and infrastructural dimensions.

## 2.2 Sneaking: A New Theoretical Framework

To make sense of children’s patterned practices of interpreting, testing, and bypassing age verification systems, we develop *sneaking* as a conceptual lens. Sneaking adapts the technical and cultural lineage of *phreaking* to the context of children’s interactions with social media age verification (Lakoff and Johnson 1980; Ludlow 2022; Warnick 2004)<sup>30,31,32</sup>. Our construction of sneaking helps us analyse how children learn the operational logics of access systems, identify weak points, and circulate practical knowledge about how those systems can be worked. To clarify what this borrowing captures, it is useful to begin with phreaking itself.

Phreaking, a portmanteau of “phone” and “freak” (1960s slang for unorthodox or free), emerged in the 1960s to describe the act, or art, of exploring, manipulating, and hacking telecommunications

---

<sup>22</sup> H. Stalford and L. Lundy (2025). *Whose business? Protecting children’s rights in the online environment*. *The International Journal of Children’s Rights*, 33(1): 1-4.

<sup>23</sup> Köhler-Dauner et al., supra note 17.

<sup>24</sup> S. Livingstone and A. Third (2017). *Children and young people’s rights in the digital age: An emerging agenda*. *New Media & Society*, 19(5): 657-670.

<sup>25</sup> A. Lavoipierre (2025). *VPNs, “old man” masks, and AI: The holes in the social media ban and their fixes*. *ABC News*, October 1.

<sup>26</sup> J. Butler (2026). *Two-thirds of under-16s with accounts on Instagram, Snapchat or TikTok kept access despite ban*. *The Guardian*, March 31.

<sup>27</sup> eSafety Commissioner (2026b). *Social Media Minimum Age: March 2026 Compliance Update*.

<sup>28</sup> Taylor, supra note 20.

<sup>29</sup> Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, supra note 15.

<sup>30</sup> G. Lakoff and M. Johnson (1980). *Metaphors We Live By* University of Chicago Press.

<sup>31</sup> P. Ludlow (2022). *Science, Metaphors, and Memes*. In: Wuppuluri, S, Grayling, AC (eds) *Metaphors and Analogies in Sciences and Humanities*. *Synthese Library*, vol 453. Springer, Cham.

<sup>32</sup> B. R. Warnick (2004). *Technological metaphors and moral education: The hacker ethic and the computational experience*. *Studies in Philosophy and Education*, 23(4): 265-281.

systems to make free phone calls or access restricted services (Levy 1984)<sup>33</sup>. Phreaks identified audio vulnerabilities in public telecommunications networks and developed techniques for using analogue signal tones to mimic operator controls. By emitting a 2,600 Hz tone into a phone, they could make the system read the line as open and route calls for free. A youth subculture grew around this practice. Young people shared tips such as using the toy whistle from Cap'n Crunch cereal boxes, which produced the right frequency; published technical information in newsletters such as YIPL/TAP (Youth International Party Line / Technological Assistance Program); and made devices such as the “blue box,” later associated with Steve Wozniak and Steve Jobs (Draper and Fraser 2018)<sup>34</sup>.

Phreaking declined in the 1980s after digital switching, including Common Channel Interoffice Signalling (CCIS), separated signalling from voice lines and made the classic tones obsolete (Gold 2011)<sup>35</sup>. Even so, phreaking is widely understood to have helped lay the technical and cultural foundations for computer hacking after personal computers and microcomputers developed in the 1970s and 1980s (Levy 1984)<sup>36</sup>. Phreaking shaped technical curiosity about opening and jailbreaking hardware and software systems. It also informed open-source ideologies and anti-corporate or anti-government critiques of computing and internet infrastructure, grounded in values of experimentation, discovery, tinkering, community, and collective knowledge sharing (Coleman 2012; Levy 1984)<sup>37,38</sup>. The practice was fundamentally playful. Although phreakers circumvented systems for practical and ideological reasons, they often did so pragmatically, seeking personal ends and shared cultural practice rather than explicit collective protest.

Building on this legacy, we coin the concept of sneaking, derived from the terms “social network freaking.” We extend the historic subcultural practice of phreaking as a conceptual lens to understand how young users perceive, interpret, and act within digital systems. Moreover, the ordinary verb to sneak names stealthy, covert, or secretive actions that avoid detection, including actions used to bypass age verification. And so, as we discuss below, the concept of sneaking carries implicit meaning and signifying capacity for thinking through emergent forms of user navigation of digital infrastructures and their governance. Like phreaking, sneaking points to personal and cultural practices of navigating and bypassing communication or security systems, here social media age verification. At a technical level, age verification systems govern access by requiring users to prove their age before entering. Much like older telephone systems, these systems have weak points, inconsistencies, and informal bypasses. Young people learn those bypasses through everyday use and develop informal expertise about system signals and operational logic. Sneaking therefore foregrounds the social tactics of discovering, developing, and distributing infrastructural knowledge.

In the context of age verification, sneaking is not a direct challenge to authority. It is a set of practices and techniques for finding vulnerabilities, evading or exploiting rules, and achieving a desired personal outcome: continued access to social media accounts. Conceptually, this aligns with materialist media theory, which treats hacking and vulnerability exploitation as foundational to contemporary computational, communication, and security apparatuses (Chun 2011; Gillespie 2018; Kittler

---

<sup>33</sup> S. Levy (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday.

<sup>34</sup> J. T. Draper and C. W. Fraser (2018). *Beyond The Little Blue Box: The biographical adventures of John T Draper (aka Captain Crunch). Notorious' Phone Phreak', legendary internet pioneer and ardent privacy advocate*. Friesen Press.

<sup>35</sup> S. Gold (2011). *The rebirth of phreaking*. *Network Security*, 2011(6): 15-17.

<sup>36</sup> Levy, supra note 33.

<sup>37</sup> E. G. Coleman (2012). *Phreaks, hackers, and trolls*. *The Social Media Reader*, 99-119.

<sup>38</sup> Levy, supra note 33.

1999; Pasquale 2015)<sup>39,40,41,42</sup>. Galloway (2004)<sup>43</sup> and Galloway and Thacker (2007)<sup>44</sup> argue that digital networks replace older hierarchical or disciplinary forms of power based on institutional authority (Foucault 2018)<sup>45</sup> with control (Deleuze 2017)<sup>46</sup>: power operates through coded systems and technical protocols that govern communication. In this framework, sneaking names technical and cultural practices that enable continued digital participation by navigating access protocols such as age verification. These practices reflect children's efforts to realise their rights and desire to participate by identifying and negotiating limits embedded in platform infrastructures and governance.

### 3 Research Methods

This study examined how children understood and responded to the restrictions in their immediate wake. Because the ban directly affected children, their accounts are central to understanding its impact. Focus groups capture contextualised and dialogic perspectives on technology use and experience (Morgan 1997; Kitzinger 1994)<sup>47,48</sup>. They also show how children negotiate shared understandings, co-construct narratives, and challenge each other's assumptions (Hennessy and Heary 2005)<sup>49</sup>. Peer-to-peer discussion is especially valuable for studying relational technologies such as social media, which operate through social expectations and group dynamics. Focus groups can also elicit examples that participants may not state publicly, including unspoken rules about what is acceptable.

We conducted five in-person focus groups with children aged between 12-16 to capture their expertise and contextualised, dialogic perspectives (Hennessy and Heary 2005)<sup>50</sup>. The focus groups took place between December 2025 and February 2026, immediately after Australia's social media age restrictions came into effect on December 10, 2025 (Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts 2025b)<sup>51</sup>. Each group lasted up to one hour and included two to four participants, with a total of 15 participants (see Table 1). We stratified groups by age (e.g., 12-14, 14-16) to support developmental appropriateness. Children were recruited through posts in school newsletters, with focus groups held at participant-chosen location. Parents or guardians provided consent, and children provided assent. The study was approved by our University ethics committee (removed for review).

---

<sup>39</sup> W. H. K. Chun (2011). *Programmed Visions: Software and Memory*. MIT Press.

<sup>40</sup> T. Gillespie (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yale University Press.

<sup>41</sup> F. A. Kittler (1999). *Gramophone, Film, Typewriter* (G Winthrop-Young M Wutz, Trans). Stanford University Press.

<sup>42</sup> F. Pasquale (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information* Harvard University Press.

<sup>43</sup> A. R. Galloway (2004). *Protocol: How Control Exists After Decentralization*. MIT Press.

<sup>44</sup> A. R. Galloway and E. Thacker (2007). *The Exploit: A Theory of Networks*. University of Minnesota Press.

<sup>45</sup> M. Foucault (2018). *Discipline*. In *Rethinking the Subject*. Routledge, 60-69.

<sup>46</sup> G. Deleuze (2017). *Postscript on the Societies of Control*. In *Surveillance, Crime and Social Control*. Routledge, 35-39.

<sup>47</sup> D. L. Morgan (1997). *Focus Groups as Qualitative Research* (Vol. 16). Sage.

<sup>48</sup> J. Kitzinger (1994). *The methodology of focus groups: the importance of interaction between research participants*. *Sociology of Health & Illness*, 16(1): 103-121.

<sup>49</sup> E. Hennessy and C. Heary (2005). *Exploring children's views through focus groups*. *Researching Children's Experience: Approaches and Methods*, 236-252.

<sup>50</sup> *Id.*

<sup>51</sup> Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, supra note 6.

**Table 1:** Participant Demographics

ID	Age	Gender	ID	Age	Gender	ID	Age	Gender
P1	13	Female	P6	12	Female	P11	13	Female
P2	14	Female	P7	13	Female	P12	16	Male
P3	15	Male	P8	16	Female	P13	15	Male
P4	14	Male	P9	14	Male	P14	15	Male
P5	12	Female	P10	15	Male	P15	15	Male

We organised the focus group discussions around four topics: (1) how children understood and perceived the social media restrictions and age verification technologies; (2) how they negotiated banned and approved social media platforms; (3) how they used digital platforms after the restrictions; and (4) how the ban affected their social lives, friendships, and wellbeing. The focus groups also included a participatory co-design activity in which children creatively and critically reimaged alternatives to the current social media age restrictions (Hourcade et al. 2023; Valguarnera and Landoni 2023)<sup>52,53</sup>. The activity moved beyond eliciting opinions by involving young participants in shaping ideas for real-world policy implementation. This approach positions children as active contributors and knowledge producers rather than passive subjects and aligns with ethical, rights-based research principles (Howard et al. 2025; Livingstone and Third 2017; Sandberg and Gille 2021)<sup>54,55,56</sup>.

We analysed the focus group transcripts using thematic analysis (Braun and Clarke 2006)<sup>57</sup>. We imported transcripts into Delve, a qualitative data analysis platform, to organise, code, and retrieve textual data and to develop analytic categories. A grounded theory-oriented coding strategy informed the analysis (Corbin and Strauss 1990)<sup>58</sup>. First, we used open coding to identify and label salient concepts and patterns in the data. We then used axial coding to compare, organise, and synthesise codes into higher-order categories, with attention to relationships between themes. To support consistency in interpretation and reflexive engagement with the data, coding decisions and the development of thematic categories were reviewed and discussed by the authors.

## 4 Findings

Our key findings capture four themes. First, young users explored and learned about age verification systems and vulnerabilities, treating checks and bans as navigable technical rules rather than absolute barriers. Second, they manipulated system requirements to bypass restrictions. Third, they developed shared vernacular knowledge about vulnerabilities in digital networks and verification systems. Fourth, they used design imaginaries to co-design alternative futures for more effective and equitable age verification. Each theme is presented below and supported by examples from our data.

<sup>52</sup> J. P. Hourcade et al. (2023). *Developing participatory methods to consider the ethics of emerging technologies for children. Proceedings of CHI*, 1-3.

<sup>53</sup> S. Valguarnera and M. Landoni (2023). *Design with and for children: The challenge of inclusivity. In Proceedings of CHI*, 171-184.

<sup>54</sup> F. Howard et al. (2025). *Researching with Young People: An Introduction to Youth-centred Research Methods. Bloomsbury Publishing*.

<sup>55</sup> Livingstone and Third, *supra* note 24.

<sup>56</sup> H. Sandberg and J. Gille (2021). *Investigating the digital media engagements of very young children at home: Reflecting on methodology and ethics. Communications*, 46(3): 332-351.

<sup>57</sup> V. Braun and V. Clarke (2006). *Using thematic analysis in psychology. Qualitative Research in Psychology*, 3(2): 77-101.

<sup>58</sup> J. Corbin and A. Strauss (1990). *Grounded theory research: Procedures, canons, and evaluative criteria. Qualitative Sociology*, 13(1): 3-21.

## 4.1 Age Verification as Platform Access Control Protocols

This theme describes how children anticipated, experienced, explored, and understood age verification mechanisms. The analysis shows that children saw platforms as the main gatekeepers for age verification and enforcement. They understood the policy through specific technical protocols, especially date-of-birth confirmation and selfie-based facial age-estimation checks. We organise this theme around two categories: children's views and experiences of platform enforcement, and their familiarity with security vulnerabilities based on prior experiences of poorly implemented social media rules.

### 4.1.1 Platform Enforcement

The social media restrictions were widely publicised, and children were acutely aware of their impending implementation. Closer to the implementation date, children received notifications to verify their age or risk losing accounts on several platforms, including the two dominant platforms discussed in the research: Snapchat and TikTok:

*"Yeah, on Snapchat, it like gave you a notification. Like, every few days it would come back, and it was like, verify your age now, or your thing will get banned" (P5, female 12)*

*"I had a little notification, like, in three days your account could be getting banned from the age thing. And then three days passed, I still have my account" (P3, male 15)*

Despite these warnings, children expressed little concern about the impact. They thought the ban was ineffective based on their initial experiences and its uneven enforcement. Many participants described not being verified at all. Others described warnings that enforcement was imminent, or cases where access was later restored:

*"Every single person I know that has gotten banned on Snapchat, they got their account back, like, after like three days" (P3, male 15)*

*"Nothing happened to me at all. ... I think for TikTok, I had my real age, but I [still] wasn't affected at all. I'm not really sure how [but] it is like a world's first, so you kind of, I wouldn't expect it to be perfect" (P13, male 15)*

*"I got banned on my Snapchat account. But then I tried to log back in, like, a week later and it just let me in" (P7, female 13)*

*"Oh, so you were banned on the actual day?" (Researcher)*

*"Yeah, like for a couple of days, but I just logged in and was let me back in" (P7, female 13)*

Many children also felt that social media companies were only superficially enforcing the ban and viewed corporate compliance as minimal, technical, profit-driven, and open to circumvention. They also recognised that platforms could still encourage under-age use by enabling access without an account on platforms like TikTok and YouTube:

*"They just do the bare minimum to make it sound like they're trying" (P5, female 12)*

*"It's because they don't want to lose their consumers" (P10, male 15)*

*"You can still watch social media without having an account. You don't need an account to use YouTube. I've got TikTok without an account. It just means you can't, like, comment or anything, or like anything or post anything" (P2, female 14)*

### 4.1.2 Security Vulnerabilities

Children's knowledge that age checks were based on self-reported birth dates or selfie-based facial age estimation, rather than physical IDs or human checking, helped them see the system as bypassable. They also recognised an asymmetry of accountability in enforcement: platforms were responsible for taking reasonable steps, while children experienced the checks as weak or hollow. Age verification was therefore understood as a technical process open to circumvention and manipulation:

*"But I think it's like a software thing that failed. Like the way that they did it. It's like matching just what someone's written, with no proof, no evidence that it's actually their birthday" (P8, female 16)*

Children's experiences and perceptions of past policies are also crucial to understanding the effectiveness of current age verification systems. Alongside their awareness of technical flaws, children described a gap between age-based platform rules and how those rules worked in practice. Some said they had already lied about age because earlier platform rules restricted children under 13 without parental permission. These prior experiences made lying about age a familiar workaround:

*"It's not gonna work, because no one puts down their real date of birth" (P8, female 16)*

*"They literally just asked me what my age was, and then there was, like, are you sure? I just clicked 'yes I'm sure' [laughs]" (P4, male 14)*

Restrictions may have failed or been circumvented technically, but children also described cases where verification worked through social norms. Access rules appeared more effective when reinforced by parental authority, perceived legitimacy, or the internalisation of norms:

*"I didn't do it [face verification] because I didn't know if mum and dad would let me ..." (P6, female 13)*

*"I didn't do it [challenge age verification] because I knew that I wouldn't 'look the part' and that I probably shouldn't push it since obviously the um rules have been put up, like, for a reason" (P11, female 13)*

Notably, no participant reported migrating to alternative platforms such as Lemon8, despite media noting this would happen, suggesting that platform value is not easily substitutable. As one participant described, "there's no kind of alternate version of TikTok" (P5, female 12).

## 4.2 Young Users Bypassing Platform Access Controls

This theme describes how young users treated age verification systems as infrastructure to be probed, tested, and worked around. In contrast to cases where no verification occurred or checks were not enforced, these accounts show children actively detecting weaknesses and developing bypass tactics. We coded these tactics into three modes: data falsification, infrastructural circumvention, and visual manipulation.

### 4.2.1 Data Falsification

Data falsification involved children deliberately utilising fake personal information to pass age gates. These forms of falsification included established exploits like entering fake birthdates, as noted above, or creating fake accounts. It also involved more responsive data and identity fabrications in response to the age ban, such as borrowing friends' accounts, or using siblings' or parents' details:

*“With the verification you can just use like a fake school ID, or you can use like your parents ID” (P2, female 14)*

*“I know some people use like, people that are older, like their cousins, and it just works” (P6, female 13)*

The use of false data can be viewed as the simplest and lowest-friction workaround, and something we have noted is already normalised in children’s routine digital practices.

#### **4.2.2 Infrastructural Circumvention**

In contrast to falsifying data, children also described tools and tactics for bypassing enforcement systems based on their awareness of platform protocols. These infrastructural techniques included the potential use of VPNs or non-banned social media platforms, although this did not eventuate because children found easier workarounds. Other approaches included account or device switching, resetting accounts after bans, using multiple accounts, and creating new accounts on the same device:

*“People could go on their iPad and make a whole new account” (P2, female 14)*

*“My TikTok account got banned, but I just made a new account, and it works ... I just said I was 16” (P7, female 13)*

Children shared experiences, discoveries, and ideas about creating multiple accounts and using different devices. These included creating a new account with a different birthday, using another household device to make a new account, or drawing on earlier experience with fake accounts. Multiple accounts helped participants reduce the risk of losing access:

*“I got banned. But I already had another account, that I’d made in case, and I just couldn’t be bothered trying to fix [the old one]” (P7, female 13)*

*“But everyone, like, just made other accounts with a new fake age” (P7, female 13)*

This mode required greater degrees of digital literacy than data falsification, though it still emerged as common amongst our participants.

#### **4.2.3 Visual Manipulation**

A particularly salient and creative mode of bypassing age verification involved manipulating images used by facial age-estimation systems. Participants described developing and applying tactics through trial and testing, rumour, peer knowledge sharing, and online searching. These tactics included asking an older relative or friend to complete age checks, holding an image of an older face to the camera, and having users of different genders and ages complete facial scans for each other:

*“Like, my little sister, her Snapchat, like, asked her to verify her age. To face scan. And I just did my face, and it was fine. I just put my face in” (P12, male 16)*

*“I know some people use like, people that are older, like their cousins, and it just works” (P6, female 13)*

*“And you can also do this, like face scans on YouTube, where it’s literally a video of, like someone doing a face scan, and you just put your phone in front of that” (P14, male 15)*

These image manipulation tactics also involved experimenting with makeup, costumes, and lighting. Children realised that lifelike verisimilitude was not necessarily important to AI image reading, so

exaggerated or humorous disguises, including fake beards, could be used to appear older even if they would look implausible to a human. Participants described how they and their friend's used creative tactics as makeup, lighting, and costuming to shape how automated systems interpreted their age:

*"She did red lipstick" (P7, female 13)*

*"Someone wore a Santa beard. And that worked" (P5, female 12)*

*"I did a face scan for Snapchat. I literally just did it in the dark, so it worked" (P4, male 14)*

*"Is that what your trick was to try to, like, dim the lighting?" (Researcher)*

*"Yeah. And then I, like, tried to make myself look as old as possible" (P4, male 14)*

*"By doing what?" (Researcher)*

*"I don't even know, looking serious. And I like, sucked in my chubby cheeks" (P4, male 14)*

These practices were often recounted with laughter, showing how humour helped render the system legible. Through such exchanges, children translated opaque computational processes into embodied, manipulable features of lighting, texture, and facial cues. This mode was a particularly advanced and creative response as platforms adopted stricter age assurance technologies.

### **4.3 Circumvention as Vernacular Knowledge Sharing**

The third theme captures how circumvention operated as a form of digital literacy within children's networks. The practices described above show that sneaking was not only individual bypassing. It was also a collective process of decoding how systems worked through shared cultural knowledge, interpretive tactics, and peer learning. Rather than simply violating rules, children developed a vernacular digital security literacy. They experienced the ban as a cohort who had previously had access, and many responded by refusing, circumventing, and sharing knowledge in order to maintain established forms of participation. We identify two categories within this theme: knowledge sharing and the ideologies underpinning the restrictions.

#### **4.3.1 Knowledge Discovery and Sharing**

In terms of information discovery and knowledge sharing around circumvention tactics they had found or heard about, children listed a range of sources, including online searching, social media feeds, school and peer-based conversations, and general rumours circulating about effective tactics:

*"Um, one of our friends did. And I've also, like, heard people online with like, the verification they can use, like, mascara, and they put like, um, like, to make it look, like, they have facial hair. And apparently, if they have any facial hair, it automatically thinks they're an adult, so I've seen people do that" (P13, male 15)*

*"We definitely get a lot of our information sources from social media" (P14, male 15)*

Children also expressed an understanding of the limitations and locus of power in enforcing the age ban, given the sense that it was ineffective. They noted the limits on platforms' ability to adhere to government policy. In contrast, children understood the home as a key site of rule enforcement and often saw parental oversight as more effective than platform-based controls:

*"It will be interesting to see if any of them actually get fined, because if they get found that they didn't take reasonable steps they can get fined \$50 million" (P11, female 13)*

*“Yeah but what is considered ‘reasonable steps’? There’s no, like simple answer to what is a reasonable step. Like they went to reasonable steps of putting in new AI to verify the age. They verified people’s ages; if they got around that, that’s on them. It’s not on the social media” (P10, male 15)*

*“I think parents have more power than, like, the actual government. Like, realistically, the government could ban you from the apps. But say your mum didn’t agree with it, she could literally take your iPad and just delete the app. The government can’t physically, like, get you fully rid of, like, all the apps they want to get rid of, but your parents can” (P3, male 15)*

### **4.3.2 Restriction Ideologies**

Children recognised the limits of enforcing the restrictions. They recognised that stricter enforcement, such as ID checks or government databases, raises privacy and practicality concerns. Some also interpreted the ban as political or ideological, seeing it as a performative response rather than a fully effective protection measure. This was further expressed in noting the limited number of platforms included in the ban:

*“So they’re [the government] just banning Snapchat, and all they’re doing is they’re like priding themselves as the first country to do it. It’s so much bullshit. There’s so much politics” (P9, male 14)*

*“I think it’s kind of weird. Like, they try to ban it, but they don’t ban half the things” (P7, female 13)*

*“Like, they don’t ban Discord” (P5, female 12)*

*“Yeah, like they banned only a few of the biggest ones. But like, what’s even the point in trying to make a ban then if there’s still half of them?” (P7, female 13)*

Taken together, these accounts point to the development of shared vernacular literacy in response to an unexpected and seemingly unfair ban. Children demonstrated an emergent understanding of how systems govern access: what data they require, how verification processes operate, where loopholes might exist, and how this knowledge can be shared.

## **4.4 Design Imaginaries for Alternative Verification Systems**

Children’s imaginaries for improving age verification systems moved beyond critique to speculative design. In the participatory co-design element of the focus groups, children articulated how systems might better align with their lived realities, implicitly proposing different configurations of trust, identity, and participation. This orientation is evident across two dimensions of their accounts: alternative verification measures, and a forward-looking belief about the benefits of the ban for future cohorts who have not yet engaged with these platforms.

### **4.4.1 Alternative Verification Measures**

When asked, “If you could redesign how age rules work online, what would you change?” participants suggested institution-based access, such as access through schools rather than birthdays. They also suggested platform-level feature restrictions. They valued limiting social media to peer interaction while curbing broader exposure to content, alongside stronger safety mechanisms to address harmful behaviour. Their proposals emphasised more nuanced, graduated forms of access rather than blanket bans, suggesting that limiting specific features would be more effective than removing platforms altogether:

*“I think it should be what grade you're in at school, because they could introduce it through the schools or something. Yeah, maybe then everyone kind of gets it at the same time instead of your birthday” (P7, female 13)*

*“And maybe not banning Snapchat completely, yeah. I feel like they can just remove features like spotlight” (P14, male 15)*

*“It shouldn't even be like a whole separate app. It should just be within the app. If you're this age, then it just, like, might restrict, like snap maps, or, you know” (P12, male 16)*

#### 4.4.2 Benefits for Future Generations

Participants framed the ban's impact as uneven across ages and cohorts. It was most disruptive for children already using social media, especially where it involved losing established accounts and social connections. By contrast, participants anticipated that future cohorts might experience the restriction as less consequential or even beneficial if access were delayed from the outset. Some suggested that a universal ban could reduce exclusion and reshape social media norms, while others saw delayed access as a way to preserve childhood and slow premature exposure to online environments:

*“I reckon if you already had it, it affects you more, but if you didn't have it, you wouldn't really care” (P6, female 13)*

*“I think that it will, like, kind of give them a minute to still be kids, and then they don't have to, like, rush into anything and, like, grow up so fast” (P11, female 13)*

*“I feel like it would work because if it banned everyone then you wouldn't be left out, you know what I mean. Then you would be like, it's, oh fine, I don't actually need it. And I think you would kind of change your perspective on social media, that you don't actually need it” (P5, female 12)*

Taken together, these design and age proposals reflect a preference for more context-sensitive and socially grounded forms of governance.

## 5 Discussion

The historical practice of phreaking is a useful starting point because it names a pattern in which security systems become legible through attempts to restrict access. Our findings show a similar pattern in children's responses to age verification: participants encountered verification as a set of practical systems to be tested, identified gaps in platform access controls, and developed and shared techniques for bypassing them. Three linked practices make up this form of sneaking. First, children encountered date-of-birth checks, inconsistent enforcement, and selfie-based age verification age-estimation systems as navigable rather than absolute. Second, they bypassed and tricked systems using false ages, new accounts, older friends or relatives, videos, lighting, makeup, and costumes to pass facial age estimation. Third, sneaking was socially learned through friends, school conversations, social media feeds, online searching, and rumours about effective tricks. This shared vernacular knowledge turned verification from a private obstacle into a collective technical challenge. Because participants could often circumvent protocols, they tended to view the ban as largely ineffective. Their workarounds, however, were not simply non-compliance. They show why age verification needs to be understood sociotechnically, as a form of infrastructural politics (Acland et al. 2015)<sup>59</sup>.

Seen this way, sneaking reframes apparent rule-breaking as testing, decoding, and navigating systems of control from within. This aligns with accounts of digital politics as immanent to networked

---

<sup>59</sup> C. R. Acland et al. (2015). *Signal Traffic: Critical Studies of Media Infrastructures*. University of Illinois Press.

systems, by finding vulnerabilities within access rules themselves, rather than opposing networks from the outside (Deuze 2011; Galloway and Thacker 2007)<sup>60,61</sup>. But sneaking also complicates exploit theory as an overtly political mode of resistance. These children were not necessarily engaged in explicit resistance or collective protest. They were pragmatically navigating systems that had made their existing social media participation uncertain. Sneaking can therefore be understood as infrastructural politics in that children recognised that platform rules, protocols, biometric systems, and organisational decisions were not neutral. They shaped who could access digital spaces and on what terms. This matters because the policy and technical decisions that governed children's access had not meaningfully included them, producing outcomes they experienced as unfair and unequal. Sneaking bridges intentional resistance and ordinary use: children may seek the practical outcome of continued access, but their collective navigation exposes the limits of technical governance.

While we use sneaking as a conceptual lens for understanding how children develop informal expertise, techniques, and communities of knowledge-sharing in the contexts of social media age verification systems, this remains one form of digital sneaking. We suggest that the concept of sneaking has wider application and significance for understanding a range of tactical forms of encounter, navigation, and deviation from the strategies of power defining digital networks (De Certeau 1984)<sup>62</sup>. The operational power maintained by digital platforms necessitates sneaking as a mode of survival, pragmatism, or politics in a range of online contexts. Just as phreaking emerged as a cultural practice in response to the dominance of large and corporate technological infrastructures, the concept of sneaking both parallels the past, but also signals to the emergence of a more diverse range of cultural practices associated with navigating digital platforms that are organised as a tightly stacked complex of technological, economic, and governance infrastructures structuring our daily lives (Plantin and Punathambekar 2019; Srnicek 2017)<sup>63,64</sup>. Sneaking is furtive, it is playful, it is experimental, and it is collective; it produces knowledge, techniques and empowerment that have potential to reorganise or reimagine the conditions of digital life, such as those of children's digital rights. Age verification protocols encode access and regulate participation through platform-controlled gates. Yet, the child-rights perspective within sneaking changes the interpretation of participants' workarounds: their testing and circumvention point to unmet claims for privacy, access, and meaningful involvement in the governance of digital environments (Livingstone and Third 2017)<sup>65</sup>. Sneaking therefore centres children as active agents within these infrastructural systems rather than passive objects in need of protection.

Participants' play, testing, and circumvention also produced vernacular knowledge. Their accounts of fake ages, account switching, peer tips, and facial-estimation tricks show that verification was understood as inputs, thresholds, and outputs that could be manipulated. Consistent with scholarship on vernacular creativity (e.g. Gibbs et al. 2015)<sup>66</sup>, this literacy was social, iterative, and collectively maintained. Further, consistent with theories of algorithmic imaginaries and folk understandings of technology (Bucher 2017; Ytre-Arne and Moe 2021)<sup>67,68</sup>, these perspectives also reveal an awareness of privacy risks associated with data-driven verification, alongside a capacity to reimagine how such

---

<sup>60</sup> M. Deuze (2011). *Media Life. Media, Culture & Society*, 33(1): 137-148.

<sup>61</sup> Galloway and Thacker, *supra* note 44.

<sup>62</sup> M. De Certeau (1984). *The Practice of Everyday Life*. Trans. Steven Rendall. Berkeley: University of California Press.

<sup>63</sup> J. C. Plantin and A. Punathambekar (2019). *Digital media infrastructures: Pipes, platforms, and politics*. *Media, Culture & Society*, 41(2): 163-174.

<sup>64</sup> N. Srnicek (2017). *Platform Capitalism*. John Wiley & Sons.

<sup>65</sup> Livingstone and Third, *supra* note 24.

<sup>66</sup> M. Gibbs et al. (2015). # Funeral and Instagram: Death, social media, and platform vernacular. *Information, Communication & Society*, 18(3): 255-268.

<sup>67</sup> T. Bucher (2017). *The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms*. *Information, Communication & Society*, 20(1): 30-44.

<sup>68</sup> B. Ytre-Arne and H. Moe (2021). *Folk theories of algorithms: Understanding digital irritation*. *Media, Culture & Society*, 43(5): 807-824.

systems might be reconfigured in more accountable and effective ways. The design suggestions extend this argument. Participants' frustrations with blanket bans were linked to alternatives such as institution-based access, parental involvement, and platform-level feature restrictions. If protocols organise participation (Galloway 2004)<sup>69</sup>, then children's proposals show an emergent capacity to imagine how those rules might be otherwise structured.

## 6 Conclusion

This paper has proposed the concept of sneaking, developed from the history of phreaking, to explain how children navigate social media age verification. The findings show children encountering inconsistent enforcement, testing verification thresholds, sharing workarounds, and proposing alternative forms of access governance. Age verification is therefore not only a technical measure. It is a negotiated digital infrastructure through which values of child trust, equality, privacy, and rights are contested. Across the four themes, children appeared as active rights-bearing agents rather than passive subjects of platform control. They learned how age gates worked, manipulated technical signals to maintain access, circulated vernacular knowledge, and imagined more nuanced, transparent, and rights-respecting forms of digital governance. Circumvention therefore operated as an everyday form of infrastructural politics, grounded in children's practical engagement with systems that shaped their digital participation. Methodologically, the focus groups made these practices visible by allowing children to explain the social expectations, peer norms, and everyday negotiations surrounding age verification. This supports a child-rights approach in which participation means more than consultation or being heard. It means recognising children as social actors and as genuine experts on their own experiences.

At the same time, sneaking has limits as a metaphor. It captures tactical navigation and informal expertise, but it should not obscure the continuing power asymmetries between children, platforms, and regulators. Platforms still control the infrastructure, even if children find temporary openings within it. Banning children from social media may also restrict access to age-relevant content and reduce opportunities for tailored engagement and parental monitoring, because platforms may design for the assumed absence of child users (Rodriguez et al. 2025)<sup>70</sup>. Focus groups also have recognised limitations. Group settings can shape what participants feel comfortable saying, particularly where peer hierarchies, pressure to conform, or sensitive disclosures are involved. Quieter or more marginalised perspectives may therefore be underrepresented. The sample also limits the study's generalisability. Participants were middle-class, urban children, and the small sample size, narrow research timeframe, and qualitative design constrain what can be inferred across socio-economic, cultural, and geographic contexts. The study does not include quantitative measures that might support statistical generalisation. Future research should address these limits by revisiting children's access to restricted social media platforms longitudinally, including parents and developers, and extending participatory co-design work that builds on children's contributions to digital technology policies that directly affect them.

## Acknowledgements

We acknowledge the Centre for Artificial Intelligence and Digital Ethics (CAIDE) for its institutional and intellectual support. We also thank the children who participated in this study for their generous contribution of time, experiences, and insights.

---

<sup>69</sup> Galloway, *supra* note 43.

<sup>70</sup> A. Rodriguez et al. (2025). *Demystifying Australia's Teen Social Media Ban*. DMRC.

## **Declarations and Funding Statement**

The authors have no competing interests to declare. This research was supported by the Australian Research Council Future Fellowship Award FT250100270, *Enhancing Ethical Design and Data Use in Child Tracking Apps*, and by Shaanan Cohny's Australian Research Council Discovery Early Career Researcher Award DE260100249, *Safe & Sound: Privacy-Enhancing Technologies to Protect Young People Online*.

## **AI Assistance Statement**

Artificial intelligence tools were used only for editorial assistance after the initial drafting of the manuscript, including cite checking, stylistic suggestions, and typesetting support. The authors reviewed and take full responsibility for all content.

## **Ethics**

This research was approved by the University of Melbourne Office of Research Ethics and Integrity. Reference Number: 2026-33398-79843-9.

## References

- Acland, C. R., P. Dourish, S. Harris, J. Holt, S. Mattern, T. Miller, and colleagues (2015). *Signal Traffic: Critical Studies of Media Infrastructures*. University of Illinois Press. (Cit. on p. 13).
- Braun, V. and V. Clarke (2006). *Using thematic analysis in psychology*. *Qualitative Research in Psychology*, 3(2): 77–101. (Cit. on p. 7).
- Bucher, T. (2017). *The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms*. *Information, Communication & Society*, 20(1): 30-44. (Cit. on p. 14).
- Butler, J. (2026). *Two-thirds of under-16s with accounts on Instagram, Snapchat or TikTok kept access despite ban*. *The Guardian*, March 31. (Cit. on p. 4).
- Champion, K. E., L. Birrell, S. Smout, M. Teesson, and T. Slade (2025). *Debate: Social media in children and young people—time for a ban? Beyond the ban—empowering parents and schools to keep adolescents safe on social media*. *Child and Adolescent Mental Health*, 30(4): 411-413. (Cit. on p. 2).
- Chun, W. H. K. (2011). *Programmed Visions: Software and Memory*. MIT Press. (Cit. on pp. 5, 6).
- Coleman, E. G. (2012). *Phreaks, hackers, and trolls*. *The Social Media Reader*, 99-119. (Cit. on p. 5).
- Corbin, J. and A. Strauss (1990). *Grounded theory research: Procedures, canons, and evaluative criteria*. *Qualitative Sociology*, 13(1): 3–21. (Cit. on p. 7).
- De Certeau, M. (1984). *The Practice of Everyday Life*. Trans. Steven Rendall. Berkeley: University of California Press. (Cit. on p. 14).
- Deleuze, G. (2017). *Postscript on the Societies of Control*. In *Surveillance, Crime and Social Control*. Routledge, 35-39. (Cit. on p. 6).
- Department for Science, Innovation and Technology (2026). *Growing Up in the Online World: A National Consultation*. GOV.UK. (Cit. on p. 3).
- Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (2025a). *Age Assurance Technology Trial: Final Report*. (Cit. on pp. 3, 4).
- (2025b). *Social Media Minimum Age*. (Cit. on pp. 2, 6).
- Deuze, M. (2011). *Media Life*. *Media, Culture & Society*, 33(1): 137-148. (Cit. on p. 14).
- Draper, J. T. and C. W. Fraser (2018). *Beyond The Little Blue Box: The biographical adventures of John T Draper (aka Captain Crunch)*. *Notorious' Phone Phreak', legendary internet pioneer and ardent privacy advocate*. Friesen Press. (Cit. on p. 5).
- eSafety Commissioner (2026a). *Social Media Age Restrictions*. (Cit. on pp. 2, 3).
- (2026b). *Social Media Minimum Age: March 2026 Compliance Update*. (Cit. on p. 4).
- Foucault, M. (2018). *Discipline*. In *Rethinking the Subject*. Routledge, 60-69. (Cit. on p. 6).
- Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. MIT Press. (Cit. on pp. 6, 15).
- Galloway, A. R. and E. Thacker (2007). *The Exploit: A Theory of Networks*. University of Minnesota Press. (Cit. on pp. 6, 14).
- Gath, M. and C. Swit (2024). *Digital media in early childhood: Risk factors for online harm and psychosocial correlates*. *Frontiers in Developmental Psychology*, 2, Article 1390276. (Cit. on p. 3).
- Gibbs, M., J. Meese, M. Arnold, B. Nansen, and M. Carter (2015). *# Funeral and Instagram: Death, social media, and platform vernacular*. *Information, Communication & Society*, 18(3): 255-268. (Cit. on p. 14).
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yale University Press. (Cit. on pp. 5, 6).
- Gold, S. (2011). *The rebirth of phreaking*. *Network Security*, 2011(6): 15-17. (Cit. on p. 5).

- Grother, P., M. Ngan, K. Hanaoka, and colleagues (2022). *Face Recognition Vendor Test (FRVT): Demographic Summaries*. National Institute of Standards and Technology, NIST IR 8429. (Cit. on p. 3).
- Hanaoka, K., M. Ngan, J. Yang, W. Quinn G, A. Hom, and P. Grother (2024). *Face Analysis Technology Evaluation: Age Estimation and Verification*. National Institute of Standards and Technology, NIST IR 8525. (Cit. on p. 3).
- Hennessy, E. and C. Heary (2005). *Exploring children’s views through focus groups*. *Researching Children’s Experience: Approaches and Methods*, 236-252. (Cit. on p. 6).
- HF, N. H. and F. An Nur (2025). *Constructing childhood realities: A communication science analysis of TikTok’s age verification failure and psychosocial impact*. *Legal Brief*, 14(3). (Cit. on p. 3).
- Hourcade, J. P., M. Alper, A. Antle, and colleagues (2023). *Developing participatory methods to consider the ethics of emerging technologies for children*. *Proceedings of CHI*, 1-3. (Cit. on p. 7).
- Howard, F., B. Hanckel, K. Moore, S. Atherton, and J. Suppers (2025). *Researching with Young People: An Introduction to Youth-centred Research Methods*. Bloomsbury Publishing. (Cit. on p. 7).
- Kittler, F. A. (1999). *Gramophone, Film, Typewriter* (G Winthrop-Young M Wutz, Trans). Stanford University Press. (Cit. on pp. 5, 6).
- Kitzinger, J. (1994). *The methodology of focus groups: the importance of interaction between research participants*. *Sociology of Health & Illness*, 16(1): 103-121. (Cit. on p. 6).
- Köhler-Dauner, F., L. Peter, E. Sitarski, K. Chauviré-Geib, A. -. C. Haag, and J. M. Fegert (2025). *Digital child protection in social networks: Age verification and age-tiered regulation in Europe* *Child and Adolescent Psychiatry and Mental Health*, 19, Article 143. (Cit. on pp. 3, 4).
- Lakoff, G. and M. Johnson (1980). *Metaphors We Live By* University of Chicago Press. (Cit. on p. 4).
- Lavoipierre, A. (2025). *VPNs, “old man” masks, and AI: The holes in the social media ban and their fixes*. *ABC News*, October 1. (Cit. on p. 4).
- Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday. (Cit. on p. 5).
- Livingstone, S. and B. O’Neill (2014). *Children’s rights online: Challenges, dilemmas and emerging directions*. In S van der Hof, B van den Berg, B Schermer (Eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Springer, 19-38. (Cit. on p. 2).
- Livingstone, S. and A. Third (2017). *Children and young people’s rights in the digital age: An emerging agenda*. *New Media & Society*, 19(5): 657-670. (Cit. on pp. 4, 7, 14).
- Ludlow, P. (2022). *Science, Metaphors, and Memes*. In: Wuppuluri, S, Grayling, AC (eds) *Metaphors and Analogies in Sciences and Humanities*. *Synthese Library*, vol 453. Springer, Cham. (Cit. on p. 4).
- Lueks, W., S. Gurses, and C. Diaz (2026). *Assessing age assurance technologies: Effectiveness, side-effects, and acceptance*. *arXiv*. (Cit. on p. 3).
- Morgan, D. L. (1997). *Focus Groups as Qualitative Research* (Vol. 16). Sage. (Cit. on p. 6).
- Online Safety Amendment (Social Media Minimum Age) Act (2024). *(Cth)*. (Cit. on p. 2).
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information* Harvard University Press. (Cit. on p. 6).
- Plantin, J. C. and A. Punathambekar (2019). *Digital media infrastructures: Pipes, platforms, and politics*. *Media, Culture & Society*, 41(2): 163-174. (Cit. on p. 14).
- Reuters (2026a). *French Senate debates social media ban for children under 15*. *Reuters*. (Cit. on p. 3).
- (2026b). *Germany’s ruling party backs social media curbs for children*. *Reuters*. (Cit. on p. 3).
- Rodriguez, A., M. Dezuanni, and E. Heck (2025). *Demystifying Australia’s Teen Social Media Ban*. *DMRC*. (Cit. on p. 15).

- Rubinstein, B. I. P., O. Ohrimenko, A. C. Cullen, S. Cohny, C. Culnane, T. Murray, M. Cheong, T. Pham, and X. Yuan (2024). *Submission 272 to the Senate Environment and Communications Legislation Committee: Online Safety Amendment (Social Media Minimum Age) Bill 2024*. (Cit. on p. 3).
- Sandberg, H. and J. Gille (2021). *Investigating the digital media engagements of very young children at home: Reflecting on methodology and ethics*. *Communications*, 46(3): 332-351. (Cit. on p. 7).
- Smahel, D., H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, and U. Hasebrink (2020). *EU Kids Online 2020: Survey Results From 19 Countries*. *EU Kids Online*. (Cit. on p. 3).
- Srnicek, N. (2017). *Platform Capitalism*. John Wiley & Sons. (Cit. on p. 14).
- Stalford, H. and L. Lundy (2025). *Whose business? Protecting children's rights in the online environment*. *The International Journal of Children's Rights*, 33(1): 1-4. (Cit. on p. 4).
- Stoilova, M., R. Nandagiri, and S. Livingstone (2021). *Children's understanding of personal data and privacy online: A systematic evidence mapping*. *Information, Communication & Society*, 24(4): 557-575. (Cit. on p. 3).
- Taylor, J. (2026). *Australia wants to sell its social media ban to the world – but are the measures even working?* *The Guardian*, April 1. (Cit. on pp. 3, 4).
- UN Committee on the Rights of the Child (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. (Cit. on p. 2).
- United Nations (1989). *Convention on the Rights of the Child*.
- Valguarnera, S. and M. Landoni (2023). *Design with and for children: The challenge of inclusivity*. In *Proceedings of CHI*, 171-184. (Cit. on p. 7).
- Warnick, B. R. (2004). *Technological metaphors and moral education: The hacker ethic and the computational experience*. *Studies in Philosophy and Education*, 23(4): 265-281. (Cit. on p. 4).
- Ytre-Arne, B. and H. Moe (2021). *Folk theories of algorithms: Understanding digital irritation*. *Media, Culture & Society*, 43(5): 807-824. (Cit. on p. 14).