NAVIGATING THE DIGITAL IDENTITY INDUSTRY

Dr Emily van der Nagel
Monash University

Digital identity integrity

Examining and explaining tensions between being public and private on the internet is an enduring aspect of the work of the Association of Internet Researchers. In this paper, I present a concept to aid those working in this space: digital identity integrity, the ability to use a range of personal accounts and platforms to meaningfully participate in digital cultures and economies.

This paper is drawn from a larger research project into digital identity integrity, and presents the results of its first two stages: establishing the discourse of the identity verification industry, and conducting pilot workshops on evaluating digital identity integrity. The project builds a case for including resistive practices to identity unification – like being anonymous or creating multiple accounts on one platform – to get a fuller picture of digital identity and inclusion.

Digital identity integrity does not mean having one online identity that is connected to civic identifiers (such as birth certificates or passports). Instead, the concept refers to the successful use of accounts that allow an individual to access the connections and communities they choose – including anonymously. Digital identity integrity is comprised of networked privacy (Marwick 2023), everyday data literacies (Burgess et al 2022), and data justice (Taylor 2017). When an individual can maintain a reasonable amount of privacy over their identity, knows how to effectively use platforms and services, and is in a position to contribute to broader digital and data justice projects, they can be said to have digital identity integrity.

The discourse of the identity verification industry

Digital identity integrity is sometimes assisted, and sometimes hindered, by the identity verification industry. This is comprised of services that promise to verify a user's age (for example, Jumio, Yoti, Veridas, and Ondato) or verify identity documents linked to an online account (for example, iDenfy, Onfido, Veriff, and SEON).

A previous investigation of a similar industry was carried out by Nora Draper (2019) on the consumer privacy industry: companies that sell privacy tools and services. Draper argues this industry and its marketing materials are an important source of discourse about what kind of autonomy individuals have over their public image. For Draper, the key tension in having an online identity is controlling the circulation of personal information while responding to the demands of cultivating a public self as a condition of participation in the digital world. This is what Alice Marwick (2013) calls the neoliberal subject: a publicly visible self that is self-configured to be watched and consumed by others. Marwick explains that a verifiable identity on social media contributes to someone's status and social capital, but these identities also benefit technology companies by making it easier to track people as they move around platforms, and collect their user data to sell to advertisers.

The first stage of this research project is a discourse analysis of the marketing material of 20 companies in the identity verification industry. It seeks to understand how these companies frame identity, privacy, and safety. For example, age-verification service Yoti (2024) calls its selfie-based age checks "accurate, frictionless and can only recognise age – not people". This marketing copy promises companies it will not invade the privacy of their customers, even though verifying age or identity requires extremely personal information. Digital rights groups like the Electronic Frontiers Foundation remain sceptical of these services, calling them "surveillance systems" and arguing that no age verification method is entirely reliable (Kelley & Schwartz 2023).

Following this discourse analysis, the research project turns to individual experiences with verification services. It will present the results of pilot workshops that consider someone's digital identity to be all their digital accounts – verified or not.

Evaluating digital identity integrity

Two pilot workshops will be conducted with a total of 40 undergraduate media students to inventory their digital identity, with the goal of evaluating their digital identity integrity – and informing formal focus groups to follow.

A short presentation on digital identity integrity will be given, followed by some small-group brainstorming of examples of how digital identity integrity can be compromised, and what the consequences of this might be. Participants will then be invited to individually, and privately, list all the platforms and apps on which they have a profile (no information about specific online profiles from any participant will be sought or recorded during the workshops). These might include social media platforms; services like email, banking, or government systems; work or student accounts; and self-quantification services like fitness apps. A discussion of whether or not participants feel they have achieved, or could achieve, digital identity integrity will then be held, with a focus on attitudes towards identity verification and resistance strategies to having one's entire digital identity connected.

Conclusion

As previous research has shown (van der Nagel & Frith 2015; van der Nagel 2017, 2018), having one unique, verifiable identity is not how most people experience the internet, or thrive within digital cultures. But for governments and technology companies, unique, verifiable identities make populations and customers easier to manage. The Australian government emphasises this in its Digital Economy Strategy 2030, which states that the government will "be succeeding when [...] the significant majority of Australians over 18 are registered for myGovID or another trusted digital identity" (Commonwealth of Australia 2021: 19).

The privacy paradox – people saying they care about privacy but providing endless personal data to platforms (Hargittai & Marwick 2016) – means that there is a disconnect between knowledge of privacy and meaningful ways to enact what historian Sarah Igo calls the "proper relationship among citizen, state, and society" (Igo 2018: 8). The goal of this research project is to work with the idea of digital identity integrity as a way to evaluate the push and pull between public and private when it comes to identities on the internet.

References

Burgess, J, Albury, K, McCosker, A & Wilken, R 2022, 'Everyday Data Literacies', pp. 83-114 in *Everyday Data Cultures*, Polity Press, Cambridge.

Commonwealth of Australia 2021, 'Digital Economy Strategy: A Leading Digital Economy and Society by 2030', Department of the Prime Minister and Cabinet, 11 May, https://apo.org.au/node/312247.

Draper, N 2019, *The Identity Trade: Selling Privacy and Reputation Online*, New York University Press, New York.

Hargittai, E & Marwick, A 2016, '"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy', *International Journal of Communication*, vol. 10, pp. 3737–3757.

Igo, SE 2018, *The Known Citizen: A History of Privacy in Modern America*, Harvard University Press, Cambridge.

Kelley, J & Schwartz, A 2023, 'Age Verification Mandates Would Undermine Anonymity Online', *Electronic Frontier Foundation*, 10 March, https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online.

Marwick, AE 2013, *Status Update: Celebrity, Publicity, and Branding in the Social Media Age*, Yale University Press, New Haven.

Marwick, AE 2023, *The Private is Political: Networked Privacy and Social Media*, Yale University Press, New Haven.

Taylor, L 2017, 'What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally', *Big Data & Society*, vol. 4, pp. 1–14.

van der Nagel, E & Frith, J 2015, 'Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of r/Gonewild', *First Monday*, vol. 20, no. 3, https://firstmonday.org/ojs/index.php/fm/article/view/5615.

van der Nagel, E 2017, 'From Usernames to Profiles: The Development of Pseudonymity in Internet Communication', *Internet Histories: Digital Technology, Culture and Society*, vol. 1, no. 4, pp. 312–331.

van der Nagel, E 2018, '"Networks That Work Too Well": Intervening in Algorithmic Connections', *Media International Australia*, vol. 168, no. 1, pp. 81-92.

Yoti 2024, https://www.yoti.com/social-media/.