Andrew Roffey
Brisbane, QLD, Australia

Committee Secretary
Joint Select Committee on Social Media and Australian Society
PO Box 6100
Parliament House
Canberra ACT 2600

4 August 2024

Submission to the Joint Select Committee on Social Media and Australian Society

Introduction

1. This submission is intended to be made public.
2. I thank the committee for the opportunity to make a submission for improving privacy, security and safety of internet users.
3. This submission mainly focuses on age verification, digital identity, social media algorithms, and other matters relating to social media.
4. Policy to improve the safety of internet users must be proportionate and balanced with security, privacy and freedom of speech.

Background

5. Bulletin Board Systems (BBS) became popular in the 1980s, supplanted by web-based internet forums and mailing lists in the 1990s to 2000s, and then massive centralised social media websites around the mid-2000s to 2010s. Federated social media (also known as “fediverse”) first came about in 2008, evolved into the ActivityPub specification in 2018, and saw massive growth in 2022. Mastodon is the most popular and well-known ActivityPub implementation as of time of writing.

Definition of social media and scope of age verification

6. Under the Social Media Services Online Safety Code, social media is defined as an electronic service that: *(i) Satisfies the following conditions: (A) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users; (B) the service allows end-users to link to, or interact with, some or all other end-users; (C) the service allows end-users to post material on the service; (D) such other conditions (if any) as are set out in the legislative rules; or (ii) is an electronic service specified in the legislative rules; but does not include an exempt service (as defined by clause 3.2).*

7. The above definition is particularly broad and all-encompassing. It likely includes services such as email, internet forums, messaging platforms and other services that might not be widely viewed as falling under the definition of social media. In the context of age verification and/or digital identification it may lead to unintended consequences.

8. Social media has overlap with messaging platforms, like Facebook and Messenger, tweets, direct/private messages, etc. Social media may also be used as a subscription platform for news, updates from organisations and entertainment. There are other centralised internet services such as Reddit and Discord which are not traditional social media websites. Reddit is largely public in nature. Discord has a mix of semi-public and private groups.

9. Social media has overlap with adjacent technologies such as mail and mailing lists, private chats and group chats, public message groups, IRC (internet relay chat), Matrix.org, XMPP, ActivityPub (Fediverse), Signal, and many others. Many of these technologies utilise open standards which do not have digital identity in their remit, and in some cases such as IRC, do not offer the capability for users to submit identity via that platform.

10. A broad scope for age verification risks overreach and unintended consequences for a wide variety of online services which Australians use.

Subversion of identity and age verification requirements by users

11. Operators of federated (fediverse) and decentralised social media technology, federated email, web technology, bulletin boards, etc. may subvert identity and/or age verification requirements. For federated social media, anybody in or out of Australia with the technical know-how can spin up an instance and invite their friends to join. Australian users can, and often do, join instances that are not hosted in Australia or operated by Australians. There are many reasons for joining an instance, often sharing knowledge in a specific or niche field, or sometimes a geographically oriented instance for a city, country or region.
12. Mastodon sites (fediverse instances) vary in size, from small sites that have dozens or hundreds of users, to larger sites nearing one million users.
13. Fosstodon.org is an example Mastodon site which is relatively large at 60,000 users and managed by a small team of geographically dispersed administrators and moderators. The site has an annual budget of nearly $40,000 for hosting costs and has no paid staff. It is hosted from the United States.
14. Most fediverse servers and internet forums are not hosted in Australia or by Australians. It is unlikely that many of these sites would implement an identity or age verification scheme for Australian users or globally. There are no technical measures in place by any actors to block Australians from joining or being invited to join this instance. Mastodon, Plemora, phpBB and other software that might fall under an age verification scheme do not have specific functionality for a country digital identity scheme.
15. Australian users may select to use VPNs, proxies or the Tor network to change their location and subvert identity and/or age verification requirements.
16. Completely decentralised social media technology, such as Secure Scuttlebutt or PZP, may be near-impossible to mandate identification and/or age verification as there is no platform or provider.

Onerous requirements on small operators

17. Digital identity and/or age verification may place onerous requirements on operators of Fediverse instances and internet forums, causing them to shut down or lose interest. Many small-time operators run servers because it's fun and interesting, but validating the age or identity of users would very likely cause many operators to turn off their instances or close registration. Small operators may have moral objections to identifying their users as it impacts their right to privacy.

Delegitimising small social media sites

18. An age verification policy which only targets massive social media websites risks delegitimising social media platforms that are not covered under the scheme or otherwise choose not to participate.

Privacy impacts of age verification

19. Requiring age verification may impact users' rights to pseudonymity as provided by the Privacy Act 1988 (Cth) and similar schemes. APP 2 states that individuals must have the option to deal with an entity anonymously or with a pseudonym. If users need to provide their identity to prove their age, the provider would need to be trained to accept an identity which does not match that in its own record.

20. Users may adopt pseudonyms for many reasons, such as a planned escape of a coerced control or domestic violence situation, giving opinions online that a user might not want associated with their employer, whistleblowing, and many other valid and lawful purposes. A scheme which inhibits or disallows pseudonyms would prevent such uses.

21. Pseudonyms are common on many social networks outside of Facebook, such as on Twitter, Reddit, Tumblr, the many fediverse instances, etc. Individuals who use a pseudonym may not want to be associated with their real name.

22. Age verification schemes may lead to hacks which expose users' personal information and making them less safe online. In June 2024 it was widely reported that a company called AU10TIX was hacked in December 2022, exposing information such as people's photo, name, date of birth, nationality, identification number, etc. This particular company was contracted by TikTok, Uber, X, and other well-known online services.

23. If a nationally operated digital identity scheme for age verification is adopted, the government or identity providers will get a record of social media websites which all users associate with, impacting peoples' privacy to associate.

24. The current national digital identity scheme, myGovID, is currently only available and supported on Google and Apple platforms.

25. Digital iD, a scheme by Australia Post poised for accreditation via Australia's Digital ID scheme, is currently only available and supported on Google and Apple Platforms.

26. Yoti, a private company referenced in the "Roadmap for age verification" paper, is also currently only available and supported on Google and Apple platforms.

27. Statistics put use of massive social media websites at over 65% usage by the total population, making social media a means of mainstream communication and entertainment.

28. Building an age verification or digital identity scheme that is exclusively provided to users of Apple and Google to the exclusion of others (LineageOS, Ubuntu Touch, Linux PC, et al.) is problematic as it makes having an Apple or Google account mandatory for a significant portion of mainstream internet usage.

29. Suggested use of Google and Apple by government through identity schemes, without interoperability, is a form of protectionism for those two companies and damages competition.

Security impacts of identity verification

30. In Australia, PSTN (public switched telephone network) methods of out-of-band or multi-factor authentication (SMS codes) have been widely adopted by government, companies and other organisations.

31. SIM and SMS (PSTN-based) hijack attacks are relatively common in Australia. Macquarie University operates an informational website called https://www.simprotect.org.au which highlights some of these attacks.

32. Outside of Australia, guidance such as NIST SP 800-63B restricts use of PSTN for out-of-band verification.

33. Australia has not adopted guidance similar to NIST SP 800-63B. Nearly all banks and financial institutions, for example, use PSTN for out-of-band verification.

34. Further adoption of identity verification on the internet without the necessary safeguards to prevent organisations using unsafe verification techniques like PSTNs risks the online security of Australians, especially in the context of proliferating identity verification for use of social media.

Government use of social media

35. Many government departments use Facebook and other social media for outreach, such as OAIC, eSafety, Bureau of Meteorology, ABC News and many others. In some of these cases, content is exclusively available on Facebook and not made available elsewhere.

36. In Canada, Facebook censors links to news websites being posted or viewed by Canadians in opposition to its version of the News Media Bargaining Code. In some cases this has prevented people from posting links about important current events like bushfires.

37. Facebook is similarly proposing to censor links to news websites being posted or viewed by Australians.

38. The Australian government's over-reliance on Facebook and Twitter for outreach and public engagement is problematic because it is beholden to the policies and interests of those companies.

39. Approaches to government use of social media by other countries could be adopted by the Australian government, such as the BBC operating its own "social.bbc" Mastodon instance which is not beholden to the policies interests of companies like Facebook or Twitter.

Privacy impacts of massive social media websites

40. Massive social media websites, such as Facebook, share personally identifiable information about users to third-party marketing vendors, analytics firms and data brokers. Many of these third parties claim to have hundreds of facts about most individuals in their databases.

41. Users are generally unfamiliar with the concept or existence of third party data brokers and unaware that they have "consented" to the disclosure or transfer of data to those organisations.

Dark patterns of massive social media websites

42. “Dark patterns” are broadly defined as user interfaces which are crafted to trick users into doing things or misleading users.

43. Massive social media websites, such as Facebook, use dark patterns to collect more information about their users, their devices, and obtain consent.

Chilling effects on free speech

44. If operators of small instances close it will impact the communities that used those instances.

45. Users may be unable to adopt a pseudonym when interacting with a social media platform, potentially limiting or preventing their speech online.

Harmful social media algorithms

46. Some social media algorithms have documented harm associated with them, most notably on Facebook, Instagram and TikTok.

47. Facebook and Instagram offer “Suggested Content” to users, which are posts and images by people or groups that they do not personally know. Suggested Content is displayed mixed in with content which the user explicitly subscribed to, such as friend, group and page updates.

48. Neither Facebook nor Instagram enable users to turn off Suggested Content in their algorithm-curated feeds.

Open APIs and interoperability

49. A “user agent” is simply software that acts on the behalf of a user, on the user’s computer, such as a web browser or email software. Every web browser and email client is a user agent. The user agent may have features like a spam filter or keyword filter in an email program, or an ad blocker in a web browser.

50. Facebook asserts that unauthorised user agents which allow users to control what they see, such as “Unfollow Everything”, a tool which allows users to unfollow all of their pages, are in violation of its Terms of Service.

51. YouTube (Google/Alphabet) asserts that users who utilise a user agent which blocks ads are in violation of its Terms of Service. It is likely that many other major operators have similar clauses.

52. Facebook does not currently provide an API which would meaningfully allow a user agent to filter content or give users more control over what they see. Facebook does provide limited controls for users to block pages and individuals one at a time, or “snoozing” an individual page for 30 days. Facebook decides which toggles to provide users as they see fit, rather than allowing fully customisable user agents.

53. User agents may empower users and give them far more control over what they see, like a spam filter in an email program. User agents may be able to offer filters for children, especially for public content.

54. User agents can be really important for people with disabilities. For example, ad blocking could be useful for blind people who use screen readers or people who have photosensitive epilepsy, both examples which barely touch the surface of uses for user agents.

55. The European Digital Markets Act (DMA) may force Facebook to open up its API, although perhaps it will only be restricted to Europeans. Australia needs its own DMA to do the same thing. An open, interoperable API may allow user agents to provide different ways of viewing social media websites and allow users to filter content which they see.

Recommendations

56. The eSafety Commissioner should not pursue age or identity verification due to its wide-ranging impacts on Australian society including privacy impacts, internet security, free speech and technical limitations.
57. ACSC should adopt Digital Identity Guidelines similar to NIST SP 800-63B which restrict use of PSTNs amongst other recommendations. Identity schemes required by the government should adopt the Digital Identity Guidelines.
58. The eSafety Commissioner should pursue toggles on social media websites to give users control over what they see, including turning off Suggested Content altogether.
59. APS should direct government departments to review exclusive use of Facebook and massive social media websites, and decouple from these sites by making content available elsewhere, especially when the content would be useful or even targeted towards school-age people. Blogs, RSS/Atom and ActivityPub are ways which content can be made more accessible, outside of massive social media websites.
60. ALRC should investigate a Digital Markets Act equivalent in Australia for many reasons, including increasing competition, forcing tech companies to interoperate and giving more control to end users.
61. ALRC's report "Serious Invasions of Privacy in the Digital Era" should be reviewed again. Mechanisms to destroy personal information (Ch.16) should be enacted to give social media users, amongst other uses, the "right to be forgotten" by websites that they no longer engage with.
62. OAIC should enforce Australian Privacy Principle 3.6 "direct collection rule" on third party data brokers. This would improve the privacy of Australians who use social media (notably), loyalty programs, bank cards, etc.
63. OAIC should investigate the AU10TIX data breach and companies using the service, and seek penalties to dissuade poor security practices which Australians are caught in as collateral damage.
64. ACCC should take enforcement action against massive social media companies for unfair terms of service, nullify user agent bans, and commit to investigate social media companies which use blanket bans on software developers that write user agents.