Australian Government

Office of the Australian Information Commissioner

Social Media (Anti-Trolling) Bill 2022 – Submission to the Legal and Constitutional Affairs Legislation Committee

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

28 February 2022

OAIC

February 2022

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Committee's inquiry into the Social Media (Anti-Trolling) Bill 2022 (the Bill). The OAIC previously made a submission to the Attorney General's Department (the Department) during the consultation on the exposure draft of the Bill.[1]

2. The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

3. The Bill proposes to establish a framework for Australians to ascertain the contact details of individuals that post defamatory material anonymously on social media for the purposes of commencing defamation proceedings. The Bill deems social media services as 'publishers' for the purposes of defamation law but includes a conditional defence to liability if the social media service discloses the valid contact details of a poster in certain circumstances.

4. We note that the Bill does not explicitly seek to prevent social media users from operating anonymously or under a pseudonym online. However, as outlined in our earlier submission on the exposure draft, a likely consequence of the Bill is that social media services will seek to collect additional contact details (if they do not already hold them) about their users and then verify the accuracy or authenticity of the details they hold so that they may access the defence to liability when required. This necessarily raises privacy risks and impacts for all Australian users of social media, which are discussed further below.

Anonymity and pseudonymity

5. Many social media services enable users to engage anonymously or pseudonymously on their platforms. Anonymity and pseudonymity are important privacy principles.[2]

6. An individual may prefer to transact online anonymously or pseudonymously for various reasons including a preference not to be identified or to be 'left alone', to avoid subsequent contact (such as direct marketing) from an entity, to keep their whereabouts secret from others, including in circumstances where they fear harm or harassment from others, to access services (such as counselling or health services) without this becoming known to others, or to express views in the public arena without fear of reprisal.[3]

---

[1] OAIC, *Exposure Draft – Social Media (Anti-Trolling) Bill 2021: Submission by the Office of the Australian Information Commissioner*, OAIC, January 2022, accessed 23 February 2022.

[2] Under Australian Privacy Principle (APP) 2, individuals must have the option of not identifying themselves or of using a pseudonym when dealing with an APP entity, unless it is impracticable for the APP entity to deal with individuals who have not identified themselves or they are required by law to deal with identified individuals.

[3] OAIC, 'Chapter 2: APP 2 – Anonymity and pseudonymity', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 17 January 2022.

7. In a recent report on the UK's draft Online Safety Bill, a parliamentary Joint Committee noted that anonymous abuse online was a serious area of concern but also acknowledged that:

> '…anonymity and pseudonymity are crucial to online safety for marginalised groups, for whistleblowers, and for victims of domestic abuse and other forms of offline violence. Anonymity and pseudonymity are not the problem and ending them would not be a proportionate response.'[4]

8. The Privacy Act recognises that the right to privacy is not absolute, and privacy rights will necessarily give way where there is a compelling public interest reason to do so. Whether this is appropriate will depend on whether any privacy impacts are reasonable, necessary and proportionate to achieving a legitimate objective.

9. The explanatory memorandum notes that where defamatory content is posted anonymously, complainants may have limited ability to identify the poster, and the capacity to seek legal recourse by bringing defamation proceedings may be limited.[5] We understand a key objective of the Bill is to empower individuals who are the victim of reputational and emotional harm to make an informed decision when deciding whether to institute defamation proceedings and, if they decide to do so, to effect service (or seek an order for substituted service) in relation to legal proceedings.[6]

10. An important threshold issue that continues to warrant further consideration is whether the privacy impact on all Australian social media users, that will result from the collection and verification of their contact details, is a reasonable, necessary and proportionate response to achieving the objective of the Bill.

11. In particular, evidence of the number of individuals that are currently unable to pursue a claim for defamation due to an inability to identify anonymous users should be appropriately balanced with the privacy impacts that may be experienced by all Australian social media users.[7]

12. In making this assessment, a relevant consideration is whether existing preliminary discovery processes to obtain information about the identity of a potential defendant in court proceedings are adequate in the circumstances.[8] These existing court processes do not incentivise collection and verification of personal information, but do enable a complainant to access information already in the possession of an entity.

13. The *Online Safety Act 2021* (Online Safety Act) also allows the e-Safety Commissioner to require a social media service (amongst other entities) to provide information about the identity of the

---

[4] Joint Committee on the Draft Online Safety Bill, *Draft Online Safety Bill – Report of Session 2021-22*, UK Parliament website, 14 December 2021, accessed 17 January 2022, p 34.

[5] Explanatory Memorandum, Social Media (Anti-Trolling) Bill 2022 (Cth), p 2.

[6] Explanatory Memorandum, Social Media (Anti-Trolling) Bill 2022 (Cth), p 8.

[7] We note that the Department's 'Frequently Asked Questions' indicate that around 1 in 7 (around 14.3%) Australians have been subjected to hate speech online, and that many report a negative impact as a result. In about 10% of cases, the negative impact is reputational damage—and this proportion appears to be higher amongst the LGBTIQ+, Indigenous, CALD and disability communities. See https://www.ag.gov.au/legal-system/social-media-anti-trolling-bill/frequently-asked-questions

[8] See for example *Kabbabe v Google LLC* [2020] FCA 126.

end user of the service and contact details of an end user of the service.[9] The Act also provides that a social media service is only required to comply to the extent they are capable of doing so.[10] This approach appears to require disclosure of the information the entity already has in its possession, rather than incentivising the collection and verification of additional personal information. We query whether the approach in the Online Safety Act could be considered further in the context of this Bill.

14. Alternatively, other avenues outside the court process may help to address the harms arising from defamatory material, such as complaints mechanisms. These can provide an opportunity for the poster or the platform to remove content, without creating a privacy risk. We note that other jurisdictions have, or are considering, a complaints scheme that leverages the channels of communication that intermediary services such as social media platforms have with the user to promote efficient dispute resolution.[11]

15. Accordingly, we recommend that further consideration should be given to whether the threshold of reasonable necessity is made out, or whether the objective of the Bill may be achieved through measures that have less impact on the handling of personal information.

Recommendation 1 – Give further consideration to the privacy impacts on all Australian users of social media services and whether they are reasonable and necessary to achieve the objectives of the Bill, or whether less privacy-intrusive options could achieve the same objective.

Additional safeguards for collection and verification of 'relevant contact details'

16. Notwithstanding the above, we have considered the substantive provisions of the Bill as currently drafted to ensure that any adverse effects of the proposed enactment on the privacy of individuals are minimised.[12]

17. Part of taking a proportionate approach is also considering what safeguards can be put in place to mitigate privacy risks. To this end, we have made several recommendations below designed to help mitigate potential privacy risks and impacts by enhancing the safeguards in the Bill. It is also important to note that the Bill does not displace the existing requirements of the Privacy Act, and social media services subject to the Act must continue to comply with their privacy obligations.

---

[9] *Online Safety Act 2021*, s 194.

[10] *Online Safety Act 2021*, s 195.

[11] See *Defamation Act 2013* (UK); *Defamation (Operators of Websites) Regulations 2013* (UK); Law Commission of Ontario, *Defamation Law in the Internet Age: Final Report*, Law Commission of Ontario, March 2020, accessed 25 January 2022, chapter IV.

[12] The Commissioner has specific monitoring related functions under the Privacy Act, which include, but are not limited to, ensuring that any adverse effects of a proposed enactment on the privacy of individuals are minimised (see s 28A(2)(c)) of the Privacy Act).

18. The Bill will deem social media services to be publishers of material posted on their platform for the purposes of defamation law. However, the Bill also includes a conditional defence to defamation liability if a social media service discloses the 'relevant contact details' of a poster either with the consent of the original poster via a complaints scheme that meets prescribed elements, or in response to an end-user information disclosure order issued by a court.

19. 'Relevant contact details' are defined in cl 6 of the Bill as:

    (a) the name of the person or the name by which the person is usually known

    (b) an email address that can be used to contact the person

    (c) a phone number that can be used to contact the person

    (d) such other details (if any) as are specified in the legislative rules (legislative rules are discussed further below).

20. We understand from the explanatory memorandum that the 'relevant contact details' are intended to be such as is necessary to effect substituted service in an Australian court and fake or inaccurate details will not meet the definition of 'relevant contact details.'[13]

21. This means that a social media service would be unable to rely on the defence if they produce fake or inaccurate details. It is also relevant to note that cl 15(3) of the Bill provides that the defence of innocent dissemination is not available to a social media service for the purposes of defamation proceedings.

22. A likely outcome of the framework set out in the Bill is that social media services will seek to collect additional categories of personal information that they do not already hold, and then take steps to verify the authenticity and accuracy of their information holdings to rely on the defence to defamation liability. Both scenarios necessarily have privacy implications.

23. As a starting point, a key privacy consideration is data minimisation, which means limiting the collection of personal information to the minimum amount that is necessary to achieve a particular objective. Data minimisation is an important privacy safeguard, which can help to reduce privacy and security risks and impacts. For example, if an entity collects more personal information than is necessary, this may increase the risk of harm to an individual in the event of a data breach. Holding large amounts of personal information can also increase the risk of unauthorised access by internal or external sources.

24. We recommend that further consideration is given to whether each of the categories of personal information listed in the definition of 'relevant contact details' is reasonably necessary in the circumstances. For instance, the definition of 'relevant contact details' could be revised so that it requires an email address *or* a phone number, rather than an email address *and* a phone number. This would further promote a data minimisation approach and may disincentivise social media services from seeking to collect additional contact details that they do not already hold.

25. A related issue is how social media services will seek to ensure that the 'relevant contact details' are authentic and accurate. The Bill is silent on this issue, however, the explanatory

[13] Explanatory Memorandum, Social Media (Anti-Trolling) Bill 2022 (Cth), p 12.

memorandum notes that 'a social media service provider is free to assess the most appropriate means of collecting personal information, in light of any incentive of the Bill, privacy obligations and commercial and practical considerations.'[14] Consequently, it is at the discretion of social media services as to the steps they will take to verify the contact details to a level of accuracy that would enable them to rely on the defence.

26. We note that a phone number and email address can be verified by less privacy intrusive methods, for example, by sending an email requesting the user click on a link to verify their account or by sending a verification code to a user's mobile phone, which must then be entered in an app or web browser.

27. However, it is not clear from the Bill whether 'the name of the person' or the 'name by which the person is usually known' in the definition of 'relevant contact details' means a person's actual or legal name.

28. If the intention is that a person's legal name is required to satisfy the definition (in order for a social media service to be able to rely on the defence), this may result in social media services seeking to collect identity information, such as government issued credentials like a driver's licence or passport, in order to verify the authenticity of an individual's name.

29. This is problematic given the privacy and security risks associated with the mishandling of this information. For instance, government issued credentials contain significantly more personal information than may already be collected and held by social media services (such as address, date of birth and other identifiers like Medicare number). Further, compromise of identity credentials and information can lead to identity theft, which has significant consequences for individuals.

30. We consider greater clarity is required around what 'the name of the person' or 'the name by which the person is usually known' means in the context of the definition of 'relevant contact details. The Bill would also benefit from greater clarity and specificity around the reasonable steps social media services should take, or the conditions they will need to satisfy, in order to be able to rely on the defence in the Bill.

31. We also recommend that additional safeguards are included in the Bill to ensure that any additional information that is collected by a social media service solely for the purpose of being able to rely on the defence, including any information collected to verify a user's name, cannot subsequently be used or disclosed for other purposes that may not align with the community's expectations. At a minimum, we recommend that the Bill includes express prohibitions on this information being used and disclosed for other commercial purposes.

Recommendation 2 – The Bill should adopt a data minimisation approach to the definition of 'relevant contact details' by, for example, amending the definition to require an email address *or* a phone number, rather than an email address *and* a phone number.

[14] Explanatory Memorandum, Social Media (Anti-Trolling) Bill 2022 (Cth) p 8.

Recommendation 3 – The Bill should provide greater clarity around what 'the name of the person' or 'the name by which the person is usually known' means in the context of the definition of 'relevant contact details, and what is required from social media services in terms of the steps they will need to take, or the conditions they will need to satisfy, in order to be able to rely on the conditional defence.

Recommendation 4 – The Bill should include additional safeguards to ensure any information collected by a social media service solely for the purpose of being able to establish the defence to liability, including any information collected to verify a user's name (such as government credentials), is not subsequently used and disclosed for other commercial purposes.

Legislative rules

32. The Bill enables additional details to be included in the definition of 'relevant contact details' if prescribed in legislative rules made by the Minister.[15]

33. A discretionary power to prescribe additional types of personal information would expand the scope of the definition and increase privacy risks if social media services are required to collect additional categories of personal information to access the defence.

34. Accordingly, we recommend that the rule-making power is removed and the definition of 'relevant contact details' is limited to what is prescribed in the primary legislation.

35. If the rule-making power in relation to 'relevant contact details' is retained, we recommend that the Department includes a provision in the Bill requiring consultation with the Information Commissioner as to whether the proposed expansion of the definition is reasonable, necessary and proportionate before any legislative rules are made, which would provide additional oversight and transparency.

36. There is precedent for such consultation requirements in other legislation for example, s 53 of the *Office of the National Intelligence Act 2018*, s 355-72 of the *Taxation Administration Act 1953* and s 56AD of the *Competition and Consumer Act 2010*.

Recommendation 5 – The ability for legislative rules to prescribe additional categories of contact details should be removed from the Bill so that the definition of 'relevant contact details' is limited to what is prescribed in the primary legislation.

Recommendation 6 – If the rule-making power in relation to 'relevant contact details' is retained, the Bill should include a provision requiring consultation with the Information Commissioner as to whether the proposed expansion of the definition is reasonable, necessary and proportionate before any legislative rules are made.

[15] See ss 6 and 32 of the Bill.

Disclosure and use of relevant contact details

37. An important privacy-preserving feature of the Bill is that social media services may only disclose a poster's relevant contact details with consent or in response to a court ordered end-user information disclosure order.

38. However, we note that the Bill does not appear to contain limitations as to how a prospective applicant may subsequently use or disclose the information they receive under the framework in the Bill. Consequently, information obtained by a prospective applicant may be used or disclosed for purposes other than commencing legal proceedings against the poster.[16]

39. As an additional safeguard, we recommend that the Bill prohibit the subsequent use or disclosure of an individual's 'relevant contact details' for purposes other than those required to initiate legal proceedings for defamation. We consider that this requirement should also be subject to a penalty to encourage compliance.

40. Relatedly, an individual may make a complaint to the OAIC if consent to the disclosure of their personal information is not properly obtained by a social media service.

Recommendation 7 – The Bill should expressly prohibit the use or disclosure of a poster's 'relevant contact details' for purposes other than those required to initiate legal proceedings for defamation and that contravention of this requirement should be subject to a penalty.

[16] The Privacy Act does not generally apply to acts or practices of individuals acting in a personal capacity. However, the Attorney General's Department's *Review of the Privacy Act 1988 Discussion Paper* included proposals for the introduction of a statutory tort for serious invasions of privacy which would enable an individual to bring civil proceedings against another individual.