

Submission to the Attorney-General

on the proposed

Social Media (Anti-Trolling) Bill 2021

21 January 2022



**DIGITAL
RIGHTS
WATCH**

General remarks

Digital Rights Watch (DRW) welcomes the opportunity to submit comments to the Attorney-General concerning the exposure draft of the *Social Media (Anti-Trolling) Bill 2021* (the Bill). DRW has been actively following the development of regulation concerned with social media and other digital platforms, especially with regard to the government's recent efforts to 'crackdown' on Big Tech. We recognise that there are unique and complex challenges posed by the ubiquitous nature of the internet and digital platforms, and the legitimate interest of the Australian government to promote safer online services to individuals across Australia.

The Bill has been framed as an "important part of the government's commitment to protecting Australians from online harms".¹ However, we are concerned that the Bill offers very little toward the protection of everyday Australians from online harms, instead focusing on increasing the power of those who elect to bring defamation proceedings, and releasing media companies from possible defamation liability. By focusing on unmasking anonymous social media users, the Bill threatens to create *additional* online harms while ostensibly seeking to reduce them.

Our key concerns regarding the Bill in its current form are:

- It incentivises social media companies to collect and store additional personal information from their Australian users in order to meet the requirement to quickly "unmask" anonymous users.
- It is unlikely to stop online "trolling", nor other forms of bullying or abuse that causes harm to everyday Australians online.
- It risks exacerbating existing power imbalances in Australia's defamation system, which may have detrimental impacts upon the quality of political speech and valid criticism of those in positions of power—a key element of a thriving liberal democracy.

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.²

¹ 'Social Media (Anti-Trolling) Bill, *Attorney-General's Department*. As at 17 January: <https://www.ag.gov.au/legal-system/social-media-anti-trolling-bill>

² Learn more about our work on our website: <https://digitalrightswatch.org.au/>
'Naming Names on the Internet,' *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>

Incentivising social media companies toward increased data collection will not minimise online harms

There is no doubt that harm takes place online by way of abuse, bullying, harassment, trolling, and defamation. These are serious issues which require significant and considered attention. We wish to emphasise, however, that the underlying business model of social media often contributes to, and exacerbates, the problem of online harm. **To that end, it is essential that any endeavour to enhance online safety or reduce harm online do not play into the hands of harmful business models.**

By offering social media companies an opportunity to avoid liability for defamatory comments posted on their platforms by way of identifying the accused user, the Bill requires social media companies to collect and store additional personal information of users. Prime Minister Scott Morrison said that “it is in the social media company’s interests to make sure they have a very voracious way of ensuring they can actually tell people who this is.”³ In other words, the government is content to give social media companies a free pass in legal terms so long as these companies collect and hand over personal information about their users.

Incentivising companies to collect and store additional personal information in order to quickly meet the requirements of the Bill creates serious privacy and security risks, which in turn can exacerbate online harms. Many of the harms caused by social media are a result of data-extractive and surveillance-based business models which rely on the collection of immense amounts of information in order to be able to target us individually, conduct hyper personalisation, and to shape, curate, and manipulate what we are exposed to online. It is clear that these practises cause significant harm to individuals, especially children and vulnerable groups. Requiring social media companies to collect and store *more* identifying details about their users favours the current model of data-hungry social media platforms and centralises sensitive information about users in a way that is not necessary or proportionate to the issue it seeks to mitigate.

Senator Michaelia Cash said that most Australians are already comfortable providing their email and phone number to social media companies, and that if the Bill “means that social media companies do require that information so they can identify you, that’s not a bad thing.”⁴ With respect, the Senator’s assessment of what users are comfortable with should not be the foundation of policy making. There is plenty of evidence to suggest that users are

³ ‘Australia’s planned anti-trolling law may silence political critics,’ *NewScientist*, 7 December 2021. Available at: <https://www.newscientist.com/article/2299944-australias-planned-anti-trolling-law-may-silence-political-critics/>

⁴ ‘We’ve had enough with trolling’: AG Cash pressures Labor on social media crackdown,’ *Sydney Morning Herald*, 20 December 2021. Available at: <https://www.smh.com.au/technology/we-ve-had-enough-with-trolling-ag-cash-pressure-labor-on-social-media-crackdown-20211217-p59ie0.html>

‘Naming Names on the Internet,’ *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>

very concerned about the privacy risks posed by social media companies and the data they collect.⁵

DRW are deeply concerned that via this Bill, the government is creating a de facto requirement for social media companies to collect additional identifying information and create a database of real identities which will be directly linked to user profiles. This generates a significant security risk. It was not long ago that Facebook experienced a data breach exposing the personal information of 530 million users.⁶ In a separate instance, ClearviewAI exploited the data available on Facebook to build a highly invasive facial recognition program, despite it being against the terms of use of the platform. By requiring social media platforms to collect and hold more information, it becomes a honeypot for nefarious actors. It is not difficult to foresee the possible harms that could occur should a social media company suffer a data breach while holding additional identifying information of their users.

Anonymity and pseudonymity online are important, and worth protecting

This Bill contributes to the current sweep of government efforts to minimise the ability for individuals to be anonymous or pseudonymous online. For example, the Basic Online Safety Expectations (BOSE) under the *Online Safety Act* contain an expectation which seeks to prevent the use of anonymous accounts.

While this Bill does not prevent individuals from creating pseudonymous social media accounts, the requirement for social media companies to be able to identify individuals means that in practice, anonymous accounts would be prohibited. It is important to note that the value of anonymity is not just in relation to an individual's identity being known by other users of the platform, it also relates to the transfer of information between individuals and the platform and the capacity of users to make a choice in this respect. It is increasingly difficult to minimise one's digital footprint, or to prevent social media companies, data brokers, and other digital platforms from creating, using and disclosing detail-rich user profiles. This Bill would exacerbate the amount of information which individuals have to trade in order to exist in the digital ecosystem—which, notably, the ongoing COVID-19 pandemic has rendered inseparable from people's everyday lives.

⁵ See 'Australian Community Attitudes to Privacy Survey 2020,' *The Office of the Australian Information Commissioner*, 2020. Available at: <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey>

⁶ 'After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users,' *NPR*, 9 April 2021. Available at: <https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users>

'Naming Names on the Internet,' *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>

Much of the rationale behind seeking to prevent or minimise people's ability to be anonymous or pseudonymous online stems from an assumption that anonymity is the root *cause* of abusive, bullying, defamatory or otherwise harmful online behaviour. In reality, there is very little evidence to suggest that this is the case in practice.

Research conducted by the Queensland Government in 2020 found that overall there was little to support the claim that identity verification would help reduce cyberbullying.⁷ In fact, their research indicated that there were significant disadvantages to imposing identity verification, including privacy risks, such as possible inappropriate secondary use of personal information.

Furthermore, following racist online abuse directed towards members of the England football team in 2021, Twitter took action to remove harmful tweets. In their subsequent analysis of the abusive tweets, Twitter found that **99% of the accounts suspended were not anonymous**.⁸ When the South Korean government imposed a law preventing individuals from posting anonymously on websites with more than 300,000 daily visitors in 2007, it was found that there was **no significant reduction in online abuse, nor prevention of spread of misinformation**.⁹ However, there was a resulting data breach resulting in 35 million South Koreans' national identification numbers being stolen.¹⁰ In other words, a significant amount of online harm is carried out not by so-called anonymous trolls but by users operating under their real names.

While there does not appear to be any significant evidence to suggest that reducing the ability for individuals to be anonymous or pseudonymous online will necessitate a reduction in online bullying, trolling, abuse, misinformation or defamation, **there are significant arguments as to why upholding anonymity and pseudonymity online is vital.**

On a societal level, anonymity and pseudonymity online play an essential role in the functionality of the free and open internet, and enable political speech online which is integral to a robust democracy. On an individual level, the ability to be anonymous or use a pseudonym allows people to exercise control and autonomy over their online identity, to uphold their privacy. Anonymity is often an essential tool to protect individual safety and wellbeing.

Any attempt to reduce the ability for people to be anonymous or pseudonymous online would undermine the above freedom and autonomy, and likely lead to increased long-term harm.

⁷ 'Social media and identity verification,' Queensland Department of the Premier and Cabinet research paper, *Queensland Government*, September 2020. Available at:

<https://www.premiers.qld.gov.au/publications/categories/reports/cyberbullying-gov-response.aspx>

⁸ 'Combatting online racist abuse: an update following the Euros', *Twitter UK*, 10 August 2021. Available at:

https://blog.twitter.com/en_gb/topics/company/2020/combating-online-racist-abuse-an-update-following-the-euro

⁹

See 'Naming names won't stop abuse on social media,' *Australian Strategic Policy Institute*, October 2021.

Available at: <https://www.aspistrategist.org.au/naming-names-wont-stop-abuse-on-social-media/>

¹⁰

'Naming Names on the Internet,' *The New York Times*, September 2011. Available at:

<https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>

We wish to emphasise that many Australians use anonymity online to protect themselves on social media and other digital platforms. Over the course of our advocacy work, DRW has heard from numerous members of the public with regard to how they use anonymity and pseudonymity online as a safety mechanism.

People who use pseudonyms online do so for a variety of reasons. For example:

- People from marginalised groups—including those from the LGBTQ+ community, disabled Australians, those from ethnic minorities—to build communities online while managing risk to their health, safety, reputation or well being.
- People seeking health information or support for stigmatised conditions.
- Victim-survivors of domestic violence.
- Whistleblowers revealing information about institutional corruption, as well as activists and human rights lawyers working on sensitive topics.
- Sex workers building professional networks which provide social support, health and safety information.
- Anyone in a public-facing role, such as social or youth workers, case managers, and lawyers, who wish to be able to maintain an online life without being tracked down or contacted by clients or those they work with.
- Individuals working in the public sector, who are generally not permitted to participate in public forums regarding politics or government positions, who wish to be part of online political discussions, including passively, without jeopardising their role or being perceived to speak on behalf of a government agency.

In 2021, DRW co-hosted an expert roundtable to explore how and why anonymity and pseudonymity online is so important. It includes Dr David Kaye, the Former United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Dr Emily van der Nagel, a researcher and expert in social media identities, platforms and cultures with a focus on anonymity and pseudonymity, among others. One of the key themes which emerged from the discussion is that research has repeatedly shown removing anonymity is not an effective method for reducing harm in online spaces. We strongly suggest the Attorney-General consider this roundtable in addition to this submission.¹¹

‘Anti-trolling’ is misleading

There are important distinctions between bullying, abuse, criticism, and defamation. We are concerned that by naming the Bill ‘anti-trolling’ it is likely to mislead Australians to believe the Bill to be something that will offer protections from more common forms of online trolling. We note that the term ‘trolling’ is not defined in the exposure draft of the Bill. This is not just an

¹¹ Digital Rights Watch and Twitter, ‘Online anonymity and pseudonymity: why it matters’, Expert Roundtable Discussion, November 2021. Available at: https://www.youtube.com/watch?v=c_g_hXCW1oY&t=1s
‘Naming Names on the Internet,’ *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>

issue of semantics. Using confusing or misleading terminology obfuscates the actual purpose of the proposed legislation from everyday Australians.

We are further concerned that in its current state the bill is so broadly drafted that it could facilitate an increase in defamation cases against ordinary Australians, including political critics and commentators. If the system set up is overly punitive to individual users, it will likely act as a deterrent to criticism and political debate online, causing people to self-censor out of fear of defamation lawsuits. This is an especially pertinent concern given that former Attorney-General Christian Porter sued the public broadcaster in defamation and resolved the matter before verdict, and the Minister for Defence Peter Dutton sued a refugee activist in a widely criticised move. Australia is widely perceived as a friendly jurisdiction for defamation plaintiffs, and there are recent examples of powerful individuals making use of this in ways that cast a chill over freedom of expression in this country.

Moreover, In the current environment it seems reckless to seek to make hurried changes to the defamation system in Australia while there is an ongoing review of defamation law currently underway.¹²

Streamlined complaints processes are needed

At DRW we support the intention to create meaningful, transparent, and accessible complaints pathways and reporting mechanisms on social media platforms. Too often these processes are overly complex, opaque, or inaccessible to everyday social media users. They are often significantly under-resourced and rarely serve basic notions of fairness.

We welcome the prospect of a legislative requirement for social media companies to streamline their complaints process. It is critical that social media companies better resource their complaints mechanisms so that the harms generated by the platform are not socialised.

None of this is inconsistent or incompatible with allowing users to remain anonymous or pseudonymous. While there may be challenges in navigating the resolution of complaints with the right to freedom of expression, these are not insurmountable. We encourage social media companies to be open and accountable when it comes to reporting on online harms and the functionality of their complaints processes.

¹² 'Review of Model Defamation Provisions,' *NSW Government*, November 2021. Available at: https://www.justice.nsw.gov.au/justicepolicy/Pages/lpcldr/lpcldr_consultation/review-model-defamation-provisions.aspx

'Naming Names on the Internet,' *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>


Recommendations

- Any legislation seeking to mitigate online harms should not rely upon reducing the ability for individuals to be anonymous or pseudonymous online, nor incentivise social media companies and other digital platforms to collect and store additional personal information.
- Any further consideration of this Bill should halt until the conclusion of the Parliamentary Inquiry into Social Media and Online Safety and the review of defamation law. The Bill should then be re-drafted with consideration of the recommendations.
- The Bill should seek not to perpetuate existing power imbalances in Australia's defamation system, which may have detrimental impacts upon the quality of political speech and valid criticism of those in positions of power—a key element of a thriving liberal democracy.
- We support legislative requirements on social media companies to improve complaints procedures, so long as they are compatible with the right to anonymity and freedom of expression

Contact

Samantha Floreani | Program Lead | Digital Rights Watch | samantha@digitalrightswatch.org.au

Lucie Krahulcova | Executive Director | Digital Rights Watch | lucie@digitalrightswatch.org.au



'Naming Names on the Internet,' *The New York Times*, September 2011. Available at: <https://www.nytimes.com/2011/09/05/technology/naming-names-on-the-internet.html>