alannah & madeline foundation

Ground Floor, 387 City Road
South Melbourne VIC 3205
Postal address
PO Box 5192
South Melbourne VIC 3205
Phone 03 9697 0666
Email info@amf.org.au
ABN 96 514 115 810
alannahandmadeline.org.au

25 March 2024

Australian Government Attorney-General's Department
Via email: Doxxing@ag.gov.au

Public Consultation on Doxxing and Privacy Reforms

The Alannah & Madeline Foundation (the Foundation) welcomes this opportunity to take part in the Australian Government's consultation on how to most appropriately address doxxing through civil remedies.

The Foundation is a leading national not-for-profit charity dedicated to keeping children and young people free from violence and trauma. We support young Australians to recover and heal from trauma; we empower them to become positive digital citizens and change the culture of bullying; and we advocate for their rights, with particular attention to the issues of firearms safety and digital technologies.

Doxxing poses risks to affected children, as the exposure of their personal information makes them vulnerable to harms such as harassment and exploitation. We welcome the Government's recognition of the seriousness of the issue and their commitment to building a safer digital environment.

Given the consultation's very tight timeframes and limited information, we cannot respond in detail. Instead, we offer the following high-level recommendations:

1. Consider the ramifications for children under 18 and engage with experts in children's rights such as the National Children's Commissioner.
2. Engage meaningfully with children and young people, including in relation to the Government's related undertaking to consult about creating a criminal offence of doxxing. Relevant bodies include eSafety's Youth Council, the Office for Youth's Youth Advisory Groups, and the Victorian Information Commissioner's Youth Advisory Group.
3. Appropriately resource the creation, implementation and monitoring of a Children's Online Privacy Code by a trusted independent regulator accountable to the public.

Doxxing affects children too

Research into children's experiences of doxxing is limited, but we know a minority of children are impacted by intentional exposure of their personal information without their consent:

- 9% of Australian children aged 8-17 said personal information about them had been posted online without their consent in the past year. (eSafety, 2022)
- 13% of US teens aged 13-17 said someone had shared their personal information online without their permission in the past 30 days. (Cyberbullying Research Centre, 2023)
- 11% of European children (15 countries) said someone had misused their personal information in the past year: 'Somebody used my personal information in a way I didn't like', 'Somebody used my password to access my information or to pretend to be me' and/or 'Somebody created a page or image about me that was hostile or hurtful'. (EU Kids Online, 2020)

A study conducted with 49 diverse teens in Australia found 'privacy issues' comprised one of their top three concerns online, including exposure of personal information and photos. (Young & Resilient Research Centre, 2021) Another survey found that while many Australian teens care about their privacy online, many also feel disempowered. 55% of teens agreed 'It's important to me that my personal information is kept private, but it's confusing and I don't really understand it'. (University of Sydney, 2023)

Meanwhile, 'Doxxing' was the second most-read article in February 2024 on the Beacon app, an Australian cyber safety app for parents provided by the Telethon Kids Institute and our partners at Dolly's Dream.

Children's experiences are different

The Australian Government has proposed to introduce a statutory tort for serious invasions of privacy, which would allow victims of doxxing to seek redress through the courts. This appears to speak to Proposal 27.1 of the Privacy Act Review Report, which the Government agreed in principle to implement.

After years of delivering digital literacy and online safety products in schools, it is our belief that children and young people would perceive barriers to accessing civil action. Few young Australians have the necessary resources. Moreover, they tend not to resolve online problems through formal means – either because they prefer to cope in other ways, do not know how to report, or do not trust reporting channels. 23% of Australian children reported their last negative online experience to the site where it occurred, while 9% reported it to the police and 8% to eSafety. (eSafety, 2022)

In our experience, when negative content is shared about children online, children's main priority is to get the content taken down quickly and then access personal support. eSafety's well-regarded cyberbullying scheme provides a means for achieving this, but unfortunately many children and parents do not know about it.

Children may also dox other people, and it is important that any legal responses to this antisocial behaviour are age-appropriate and recognise children's early stage of development and potential for positive growth. This point may be more relevant to a potential future criminal offence for malicious re-identification of de-identified information, as proposed in the Privacy Act Review Report (4.7) and agreed to by the Government. When responding to offences by children, rehabilitation and behavioural change should be prioritised and heavily punitive responses are unlikely to be appropriate. Many children who behave antisocially online have also been targeted themselves. For example, a study of doxxing among adolescents in Hong Kong found a strong overlap between perpetration, victimisation and bystanding. (Chen et al, 2019)

Children's voices should be heard and their rights upheld

As an organisation dedicated to upholding children's rights, we note Article 16 of the United Nations Convention on the Rights of the Child (UNCRC): 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation … The child has the right to the protection of the law against such interference or attacks.'

This right coexists (and must be balanced) with others, including children's rights to access information and material from a diversity of sources and to seek, receive and impart information freely, subject only to such restrictions necessary to protect the rights or reputations of other people.

Children also have a right to express their views freely on matters that affect them, thus giving policymakers a clearer picture of children's strengths, vulnerabilities and priorities, which may differ from those of their elders. Child and youth engagement also aligns with the Safety by Design principle of user empowerment and autonomy championed by the eSafety Commissioner.

Unfortunately, the 17-day timeframe for this consultation makes meaningful child and youth engagement unlikely, but we encourage consultation with relevant youth advisory bodies, such as eSafety's Youth Council,

the Office for Youth's Youth Advisory Groups (eg. Civic Engagement, First Nations), or the Youth Advisory Group of the Victorian Information Commissioner.

This current consultation does not appear to address the Government's related agreement to consult on introducing a criminal offence for malicious re-identification of de-identified information, in line with Proposal 4.7 of the Privacy Act Review Report. (Presumably the Government's public undertaking to introduce a criminal offence for doxxing was made in reference to this.) We trust this means the Government has more time to plan for child and youth engagement on the topic of criminal sanctions for doxxing.

Safety by design helps to prevent harm

Malicious exposure of personal information online is made easier through weaknesses in many digital platforms, whose commercial model is based on maximising user engagement and handling of user data. If platforms protected children's personal information better, we believe many risks would be reduced.

The Foundation applauded the Australian Government's commitment to create a Children's Online Privacy Code akin to the UK Children's Code. Requirements to industry might include:

- Switch geolocation off by default unless there is a compelling reason to do otherwise, taking account of the best interests of the child.
- Make it obvious to children when their location is being tracked.
- Revert any settings which make a child's location visible to others to 'off' after each use.
- Set children's accounts to 'high privacy' by default unless there is a compelling reason to do otherwise, taking account of the best interests of the child.
- If children lower their settings, give them the option of restoring high privacy defaults after a session.
- Do not 'nudge' children to provide unnecessary personal information or turn off privacy protections.
- Make the platform's privacy information concise, prominent, clear, and age-appropriate.
- Provide prominent, accessible tools to help children report any concerns and exercise their data protection rights.

If implemented, such measures would speak to one provision of the Government's anti-doxxing consultation: to 'give individuals greater control and transparency over their personal information'.

To deliver such protections to children in Australia, we believe Code development should be led by a trusted independent regulator accountable to the public. Appropriate resourcing must be in place to enable the regulator to engage and advise industry, monitor adherence, and investigate and address any serious or systemic failures to comply. From what we gather of the UK experience, it appears industry adherence has been uneven and intervention by the regulator continues to be necessary.

We would welcome the opportunity to discuss any of these matters further with you.

Yours sincerely,

Sarah Davies AM
Chief Executive Officer