



28 March 2024

Online Hate Prevention Institute submission to the
Attorney General Department's Public Consultation on Doxxing and Privacy Reforms

About this submission

This submission is from the Online Hate Prevention Institute, an Australian Harm Prevention Charity established in January 2012 with a focus on online hate and extremism. This submission is prepared by our CEO, Dr Andre Oboler.

General Principles on Privacy applied to doxxing

Australia has no tort for serious invasion of privacy. It is not part of the common law and if it were to be created, it would need to be done through legislation. The Law Council of Australia has expressed support for the creation of a statutory tort for serious invasion of privacy.¹ We support this position.

From a doctrinal position we believe that as far as possible the law should follow the *principle of generality* which holds that “where possible existing laws which are not specific to the online environment should be relied upon”.²

This means doxxing should first be addressed in a manner that is format neutral. Whatever is deemed to constitute doxxing should apply whether the information is published online, broadcast on television, printed on flyers or banners, or circulated in any other form.

The nature of the online environment can, however, significantly change the “nature of the conduct or its prevalence”,³ which means a criminal response may be warrant for online activity in cases where it would not be criminal when engaged in offline.⁴

We recommend including both a general provision, and particular laws to address the specific nature of the online world, for example penalties for platforms that fail to take reasonable steps to prevent the acceleration of harm through their platforms, and heavier penalties for social media influencers who engage in doxxing as their use of social media for commercial purposes, and reach, should come with a greater responsibility to ensure their activities don't cause harm.

By social media influencers we refer to those with large followings on their accounts, whether they are individuals, brands, mainstream media organisations. We would urge that politicians and political parties

¹ <https://lawcouncil.au/media/media-releases/law-council-supports-statutory-tort-for-serious-invasion-of-privacy>

² Andre Oboler, “Legal Doctrines Applied to Online Hate Speech”, *Computers & Law*, July 2014.

<https://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>, p 9—10.

³ Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2010) 16.

⁴ Andre Oboler, “Legal Doctrines Applied to Online Hate Speech”, *Computers & Law*, July 2014, p 9—10.

<https://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>



be explicitly included in the coverage as there are no valid grounds for an exemption and the existing exemptions in the privacy act have been abused.⁵

In 2022 a submission from the eSafety Commissioner detailed “publishing private or identifying information about an individual with malicious intent to cause serious harm” and “‘volumetric’ attacks, also known as pile-ons or brigades” as two distinct forms of the “most serious types of abuse targeting adults”.⁶ The risk we have seen recently is the combination of these two harms, greatly accelerated by social media influencers, and carried out against not one individual but large numbers of individuals that form a group identifiably by a protected characteristic. Consideration should be given to greater penalties in the case of a crime related to doxing also being a hate crime.

Case studies and considerations

We present the following case studies as a basis to discuss ideas of what should or should not be covered by a new law on doxxing and wider considerations in this space.

Case 1: The Jewish Artists and Creatives List

The conversation from a private WhatsApp group of Jewish artists and creatives was published along with a spreadsheet containing details on the group members. The spreadsheet listed their names as they appeared in the chat, their real name (sometimes adding a full name to what was a nickname), profession, position, company, accounts on a range of other social media platforms (LinkedIn, Instagram, Facebook, Twitter), details on their activity in the group and notes that often included their relationship to others.

Not all details were provided for all members, 113 of them had at least one social media account which could be used to contact them listed. The list did not include phone numbers or physical addresses, but with the names some of those details could be easily found from the White Pages. It is also unclear to us if the people who initially extracted the list infiltrated it for this purpose or had been legitimate members of the group who then turned on it.

The list went viral when shared by a social media influencer with significant reach (over 200,000 followers) and a history of instigating volumetric attacks against anyone who criticized her – even in private messages to her. The result was harassment of members of the group using their social media accounts, as identified in the spreadsheet. One family had to go into hiding.⁷

On one of the influencers posts that went viral, concerns were expressed for the impact that sharing the information could have on the safety of those listed. The influencer was aware of this concern and unconcerned about the potential harm her actions could cause. The post was also removed by the social media platform and simply reposted, showing a rejection of the platforms efforts to protect people’s

⁵ Andre Oboler, “Tim Wilson’s ‘retirement tax’ website doesn’t have a privacy policy. So how is he using the data?“, *The Conversation*, 8 February 2019. <https://theconversation.com/tim-wilsons-retirement-tax-website-doesnt-have-a-privacy-policy-so-how-is-he-using-the-data-111076>

⁶ *eSafety Commissioner Submission to the Inquiry into Social Media and Online Safety*, January 2022. <https://www.esafety.gov.au/sites/default/files/2023-04/eSafety-submission-Inquiry-into-social-media-and-online-safety.pdf>

⁷ <https://www.theguardian.com/australia-news/2024/feb/12/albanese-government-to-propose-legislation-to-crack-down-on-doxing>



safety and of another warning that the post may be putting others at a risk. One person commented on the post saying they were concerned the list could be used by neo-Nazis to target Jewish people, another replied that the point was not for neo-Nazis to target those listed but for others to be able to target them.⁸ This targeting was described as the point of sharing the information. It reflects a broader issue of “Racist Anti-Zionism” a form of antisemitism in which attacks on the Jewish community are currently being justified.⁹ The social media influencer was actively engaged in the conversation and it seem highlight likely she saw this conversation, another warning about the potential harm.

General law considerations

- The conversations were in a private group. If there was a tort of privacy, it might cover leaking the conversations themselves. This is a broader issue about private conversations and could be handled at a higher level not specifically related to online activity. It may be considered legitimate (and protected) for a person in a private conversation to share details of the conversation. It may be considered illegitimate (and not protected) if they were only in a position to hear the conversation due to false pretences or outright fraud (which may negate the protection).
- There might be an exception for journalism if quoting newsworthy comments from a private conversation. There may need to be safeguards around this, for example ensuring it is professional journalist acting in the course of their work.

Technology law considerations

- In the specific context of online conversations, consideration needs to be had on whether infiltrating an online group under false pretences and using an electronic device to then gather conversation and users, turns that device into an electronic surveillance device which should be subject to the same laws that prevent wiretaps. A consideration is whether this only applies when a technical means is used, or if it also applies when social engineering is used.
- Those with significant reach online (including public figures, brands, mainstream media, and social media influencers) need to be held to a higher standard as they can cause greater harm. They also use social media for advantage (often financial) which can create added incentive to engage in conduct harmful to others. Professional ethics in fields like journalism seek to curb such harms, but not all with influence and reach online are subject to such ethical codes.

General or technology considerations

- A particular feature in this case is the creation or exacerbation of a risk of harm to others. The publication by the social media influencer, despite them not creating the content, might be considered either negligent (failing to consider the potential harm), or a form of incitement to harm and facilitation of it. The likely harm might include physical harm (as the details provided could be used identify people’s residential addresses in some cases), or the greatly increased risk of online harassment including volumetric attacks.
- It is the publication of the details in a specific context which is the issue and differentiates it from normal conversation where a person’s online account might be linked.

⁸ <https://ohpi.org.au/targeting-jews-is-antisemitic/>

⁹ Oboler, Roth, Beinart & Beinart (2024). Online Antisemitism After 7 October 2023. Online Hate Prevention Institute. <https://ohpi.org.au/afteroct7/> see pages 203-208.



- The context includes people being targeted simply for being a member of a group, and in this case a group that is partly defined by a protected attribute. The issue of doxxing as a hate crime needs to be considered and potentially given higher penalties.

Case 2: Identification of a neo-Nazi

On January 22, 2024, the Online Hate Prevention Institute shared a confidential report identifying an individual with a range of government agencies including the Home Affairs, eSafety, the Australian Human Rights Commission, and South Australian Police, our contacts at a number of social media platforms, and a very small number of community leaders.

The person was neo-Nazi whose social media posts across two social media platforms repeatedly called for Jews to be killed in very explicit terms. This person was a lone operator and not part of a well-known neo-Nazi group. We believe they pose a violent extremism risk to the public in general, and to the Jewish community in particular. They were also, in our view, unlikely to unknown to authorities.

Our briefing included details of their name, home address, workplace, photographs, social media accounts on multiple platforms, and examples of what they had been posting that was cause for concern.

We did not publish any identifying details in public. When publishing an example of the concerning content, we redacted both the username and the profile picture of the poster.

Some would call out the content in a manner that identifies the account it is comes from, for example by replying to it and labelling it as racist, inciting violence, etc. They might tag a police force like the AFP or an agency like eSafety when doing so. This is a normal use of social media, replying in a public conversation to content that has been posted in public. On some platforms (e.g. Facebook) the person who posted the original content can remove their post and the replies will also vanish. On others (like Twitter), deleting their post will not remove the reply, but would remove the context, and the reply will show it is in response to the deleted post.

General law considerations

- Constraining the work of non-government organisations that work in the CVE space would harm public safety. To prevent abuse, exemptions might need to be limited to registered charities, or specifically to the more limited and tightly regulated set of Harm Prevention Charities.
- An exemption for law enforcement or supporting law enforcement is insufficient:
 - Government agencies like the Australian Human Rights Commission or eSafety may have a non-law enforcement capacity in which such information is useful. Policy areas in other parts of government may also have a legitimate interest in such information.
 - Where a particular community is at risk, its peak bodies need to be informed in order to manage that risk.
 - To mitigate risk, a venue or business may need to be informed of a threat.



Technology law considerations

- The online publication of concerning content, absent personal information, should not be prevented as it is needed to raise awareness and educate against such behaviour.
- Replying in public to a post that was made in public, and referencing the poster, is a normal part of online engagement and should not fall into doxxing laws.

Case 3: Documenting public content

The online hate prevention institute has published hundreds of articles document online racism and other forms of online hate. Our normal practise is to redact the usernames and profile pictures from the images we share. Doing so identifies the hate without identifying the account that posted it.

In some cases, we provide links to the problematic content and encourage people to report the content to the platform provider. This does identify the account involved and while the action we advocate is platform reporting, it can be used by others to reply to the poster of the content. We routinely engaged in this form of activity when we first started in 2012, but have done so far more rarely in recently years, normally only in the case of truly anonymous accounts that are used primarily for spreading hate, or in the case of accounts belonging to public figures.

This approach is taken out of an abundance of caution given the potential harm that could be caused by an online mob seeking to undertake a volumetric attack in response to racist content or other forms of hate speech. This approach does lead to far lower engagement with our work than if we were naming and targeting racist accounts as other organisations in Australia and overseas do.

A key feature of our publication of screen captures of harmful content is that, unlike when social media is embedded or linked, with a screen capture the person who made the post has no ability to remove the content. Deleting their original post will not impact our image of it in anyway. In our case, with the content anonymised, this is not significant. Those who do not redact personal information may be publishing content document that e.g. a person was once racist online, in a manner that could have a long-term impact on the original poster, even if they stop engaging in racism.

General law considerations

- Where personal information is used, consideration needs to be had to the individual's right to be forgotten compared to the public interest. A careful consideration of GDPR and the implications in Europe of that approach should be considered in selecting the right balance of rights for Australia.

Case 4: response to a vile video

Following an arson attack on a fast-food restaurant owned by a Palestinian activist, a young Jewish man filmed a social media video outside the venue where he made a number of vile comments. The video caused outrage among pro-Palestinian activists who shared links to it with numerous people calling for him to be found. His name and social media accounts were shared on multiple platforms, a former employer was targeted and put out a statement, an image with a range of personal details was circulated.



We recall seeing an image with more detailed doxxing, possibly with a home address included. The video was cited as one of the reasons for a pro-Palestinian protest that turned violent. The doxxing and online targeting led the young Jewish man, who it later emerged has mental health issues, to jump off a multi-storey building to commit suicide. He was in hospital on life support for a time and then passed away.

Online people continue to call for the family to be targeted and claimed the news of his hospitalisation and then death were “fake”. This occurred even after pictures were shared of him in hospital, and even after the owners of the burger store called for the harassment to stop. A picture of a message from the man’s father to the burger store owner showing him in hospital and apologising for the video his son had made was circulated to support the family, but inadvertently included the father’s mobile number.

General law considerations

- Details of the video were newsworthy and discussed in the media. In this context the name and possibly an image of the person speaking into the camera might be considered relevant.
- Calls to “find” or identify the person in the video are calls for doxxing. This itself we considered an offence.
- The calls to doxx the person were at times combined with calls to use this information to attack the person. This is beyond simple doxxing and consideration should be given to an offence related to calling for doxxing while inciting violence against the victim.

Technology law considerations

- Responding to the video when originally posted would have been reasonable.
- Sharing other social media accounts on other platforms, particularly platforms like LinkedIn which listed further personal details such as real names, employers, education, potential contact details, can be a form of doxxing and quite distinct from normal social media usage.
- The intent of linking to other social media accounts is important, as linking to a post on one platform from another can also be a normal part of online activity.
- The accidental sharing of personal information, for example the phone number in this case, should not be considered doxxing.

Other matters

Elements of an offence related to doxxing also need to consider:

- The purpose for which the information is shared.
 - It may be acceptable to encourage people to respond in outrage to a particular post by a particular account.
 - Once the problematic contents is removed, or the account closed or made private, continuing to pursue the person on other channels or offline may be a form of stalking. Sharing information to facilitate such stalking may be a form of doxxing.
 - Any further action should be taken through proper channels and not by a mob. E.g. reporting to police, other government agencies (e.g. eSafety, Australian Human Rights Commission, etc), community representative bodies, or other civil society organisations.



- The distinction between public and private may not be sufficient
 - While public and private spaces can make sense in the physical environment, the concept is less well defined online. If doxxing were only to apply when content was made public to the world, such details could still be shared to large groups and between such large groups, that allowed people to be targeted – all without it being public.
- A public interest exemption should exist, but should require reasonable steps to minimize harm.