Executive Council of Australian Jewry Inc.

הועד הפועל של יהודי אוסטרליה

The Representative Organisation of Australian Jewry

[redacted]

Address all correspondence to:
PO Box 1114, Edgecliff NSW 2027

Tel (+61 2) **8353 8500**
Fax (+61 2) **9361 5888**
Web: www.ecaj.org.au
E-mail info@ecaj.org.au

PRESIDENT
Daniel Aghion KC

DEPUTY PRESIDENT
Robert M Goot AO, SC

IMM. PAST PRESIDENT
Jillian Segal AO

HON. TREASURER
Peter Wise AM

HON. SECRETARY
Anton Block AM

Co-CEOs
Peter Wertheim AM
Alex Ryvchin

VICE PRESIDENTS
David Ossip (NSW)
Philip Zajac (VIC)
Geoff Midalia (WA)
Jason Steinberg (QLD)
Annetay Henderson-Sapir (SA)
Jeff Schneider (TAS)
Athol Morris (ACT)

CONSTITUENTS
NSW Jewish Board of Deputies
Jewish Community Council of Victoria Inc
Jewish Community Council of Western Australia Inc
Queensland Jewish Board of Deputies
Jewish Community Council of South Australia
Hobart Hebrew Congregation
ACT Jewish Community Inc

AFFILIATES
Australasian Union of Jewish Students
Australian Federation of WIZO
Union for Progressive Judaism
Federation of ~~Jewish~~ Aged Care Services
Maccabi Australia Inc
National Council of Jewish Women
B'nai B'rith of Australia/ NZ
Jewish National Fund of Australia
Joint Distribution Committee Australia

OBSERVERS
Council of Progressive Rabbis
Federation of Australian Jewish Ex-Service Associations
New Zealand Jewish Council
Zionist Federation of Australia
Council of Orthodox Synagogues of Australia

21 June 2024

Ms Delia Rickard PSM
The OSA Review Secretariat
Online Safety Branch - Online Safety, Media and Platforms Division
The Department of Infrastructure,
Transport, Regional Development,
Communications and the Arts
GPO Box 594, CANBERRA ACT 2601

By email: OSAReview@COMMUNICATIONS.gov.au

Dear Ms Rickard

Submission to the Statutory Review of the Online Safety Act 2021

Introduction

The Executive Council of Australian Jewry (the ECAJ) is the peak, elected, representative body of the Australian Jewish community. We make the following submission in response to the independent statutory review of the *Online Safety Act 2021* that is being conducted by the OSA Review Secretariat Online Safety Branch - Online Safety, Media and Platforms Division. This submission is also made on behalf of the ECAJ's Constituent and Affiliate organisations throughout Australia.

The ECAJ has been tackling online hate since the 1990s. The Federal Court judgments in the legal proceedings pursued by the ECAJ from 1996 to 2009 against the Australian based Holocaust denial website, the Adelaide Institute, and its founder Fredrick Toben[1], have had a significant impact on the way Australia understands and approaches the problem of online safety.[2] For thirty-five years, the ECAJ has published annual reports on antisemitism in Australia which have also documented online antisemitic content, including the use of social media to spread hate and extremism by individuals and hate groups.

In 2015 a project by the Online Hate Prevention Institute (the OHPI), supported by the ECAJ, used Australian technology and expertise to create the world's first empirical report on social media antisemitism. The report highlighted how 10

[1] *Toben v Jones* [2003] FCAFC 137 (27 June 2003); *Jones v Toben* (includes explanatory memorandum) [2002] FCA 1150 (17 September 2002)
[2] *At a glance: Racial vilification under sections 18C and 18D of the Racial Discrimination Act 1975 (Cth),* Australian Human Rights Commission: https://humanrights.gov.au/our-work/race-discrimination/projects/glance-racial-vilification-under-sections-18c-and-18d-racial

months after being reported, most social media antisemitism remained online. For some types of antisemitism on some platforms, over 90% remained online.[3]

We believe that on certain platforms the most seriously harmful material tends to be removed more expeditiously than it was in the past, but the volume of such content has increased dramatically, and there is a long way to go. The ECAJ's annual antisemitism reports show that antisemitism, even amounting to criminal conduct, continues to be visible all over social media in Australia.[4] As the Minister for Communications, the Hon Michelle Rowland MP, noted in a speech on 22 November 2023, online interactions have expanded the vectors for harm and their ability to scale.[5]

The ECAJ believes that the current gaps in the *Online Safety Act 2021* ('The Act') and particularly its failure to address online harms inflicted on protected groups,[6] is a major reason why a permissive environment for antisemitic discourse has flourished online, contributing significantly to an increase in such discourse both online and in the physical world. This permissive environment has contributed to the dramatic rise in the number of reported antisemitic incidents.[7] In fact, the online environment contains such a massive amount of antisemitic material that the ECAJ excludes online antisemitic discourse from its tally of incidents in its annual reports.[8]

Our submission seeks to address the ten specific matters outlined for consideration in the Review Terms of Reference, but all aspects of our submission should be read in the context of our overarching contention that at present there is insufficient protection online for vulnerable groups, and timely reform is necessary to correct this.

Specific matters to be considered by the Review

1. **The overarching objects in section 3 of the Act, including the extent to which the objects and provisions of the Act, remain appropriate to achieve the Government's current online safety policy intent.**

The remit granted to eSafety to date has not been broad enough. Although the objects of the Act are to improve and promote the safety of Australians online,[9] the current regime focuses on limited categories of regulated harms that include child cyberbullying, adult cyber-abuse, the non-consensual sharing of intimate images, illegal and restricted content and material depicting abhorrent violent conduct.

---

[3] Oboler, Andre, *Measuring the hate: the state of antisemitism in social media*, Online Hate Prevention Institute, January 2016: https://nla.gov.au/nla.obj-1971821446/view

[4] Nathan, Julie, *Report on antisemitism in Australia 2023*, Executive Council of Australian Jewry, 1 October – 30 September 2023: ECAJ-Antisemitism-Report-2023.pdf

[5] The Hon Michelle Rowland MP, Minister for Communications, Online Speeches, Address to the National Press Club 22 November 2023: https://minister.infrastructure.gov.au/rowland/speech/address-national-press-club, accessed 20 June 2024.

[6] 'Protected groups' is used in this document to refer to groups of any 'race, colour, descent or national or ethnic origin', for which it is unlawful to discriminate against under the Racial Discrimination Act 1975 (Cth).

[7] *Preliminary statistics concerning surge in antisemitic incidents following Hamas atrocities in Israel on 7 October 2023*, Executive Council of Australian Jewry, 15 December 2023.

[8] see Nathan, Julie, *Report on antisemitism in Australia 2023*, Executive Council of Australian Jewry, 1 October – 30 September 2023: ECAJ-Antisemitism-Report-2023.pdf, pp. 34.

[9] *Online Safety Act 2021*, Section 3.

The legislation does not cover other areas including online hate, volumetric (pile-on) attacks, or technology-facilitated abuse. It also does not specifically address incitement of violence or hatred towards groups.

Changes introduced during 2021 have expanded eSafety's remit, and the ECAJ welcomes that, but vulnerable communities are still not sufficiently protected. The targeting of the Jewish community as a whole with unlawful hate speech is neither an attack on a child, nor an attack on an adult, yet it impacts adversely upon both.

In 2022, the House of Representatives Select Committee on Social Media and Online Safety heard evidence about online harm and reported, among other things, that some groups of Australians are more likely than others to experience online harm or the effects of dangerous online behaviour. The groups facing an elevated risk include people from culturally or linguistically diverse backgrounds and people with particular religious beliefs.[10] The current eSafety framework does not take into account the need for additional oversight and protection with respect to these groups, including the Jewish community.

Furthermore, while there are some advantages to a systems-focussed approach to preventing online harm, it is not in the interests of industries to push for tougher self-regulation under the Basic Online Safety Expectations (BOSE) or the Industry Codes and Standards. Although some service providers have invested in AI to remove harmful content automatically, their terms of use, Industry Codes and Industry Standards still place the burden of responsibility on users to determine whether there has been a breach, and to take action.

This leads to anomalous and at times perverse results. For example, the online publication of images and videos that include abhorrent violent content perpetrated against Jews as a group, including the rape and torture of victims of the 7 October massacre perpetrated by Hamas, would likely lead to the removal of such content under the regulatory regime; yet it is permissible for individuals and organisations to use online spaces to deny that the atrocities occurred, or to belittle the victims, and to spread antisemitic conspiracy theories to try to explain away the abundant online and other evidence of these crimes. [11]

Recommendation 1: That the overarching objects in section 3 of the Act be amended so as to provide explicitly for the improvement and promotion of online safety for individuals *and protected groups*.

2. **The operation and effectiveness of the following statutory schemes and whether the regulatory arrangements should be amended:**
   - **cyber-bullying material targeted at an Australian child**
   - **non-consensual sharing of intimate images**
   - **cyber-abuse material targeted at an Australian adult**

[10] Social Media and Online Safety, House of Representatives Select Committee on Social Media and Online Safety, 'Social Media and Online Safety' (March 2022), 29 – 44, Social Media and Online Safety (aph.gov.au), accessed at 28 May 2024.

[11] See for example, Abdel-Fattah, Randa, 'A critical look at the *New York Times* weaponization of rape in service of Israeli propaganda', *Institute for Palestine Studies*, January 2024: https://www.palestine-studies.org/en/node/1655054

- **the Online Content Scheme, including the restricted access system and the legislative framework governing industry codes and standards, and**
- **material that depicts abhorrent violent conduct**

- **Cyber-bullying material targeted at an Australian child or at an Australian adult**

In early February 2024 a list of 600 Jewish Australian artists and creatives who were on an informal Whatsapp chat group was published, along with excerpts of their private conversations and a spreadsheet that included the names, phone numbers, social media profiles and images of the chat group members. In some instances personal data of Jewish children and their images were published online in what is known as "doxing".

Prime Minister Anthony Albanese and Attorney-General Mark Dreyfus noted that the doxing had deliberately targeted these individuals "because they happen to be Jewish".[12] The incident illustrated the current gaps in the *Online Safety Act 2021*. In the case of some of the children whose images and data were published, the Section 6(b) conditions may not have been met, as the intention of those publishing the data may have been to cause harm to the Jewish group as a whole rather than to any particular child whose data was shared. It might also have been difficult to prove that "*the material would be likely to have the effect on the Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child*", even though the material obviously compromised the children's privacy and security. Similarly, regarding the adults who were doxed, it may have been difficult to prove under section 7(b) of the Act, that "*it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult*," as arguably the intention of the doxers was not directed at any one of the particular adults but rather at silencing the group.

The online spreadsheet and images were removed fairly quickly, although it is unclear if the doxers did this in response to a request of the eSafety Commissioner or of their own volition. However, the damage was done and the doxing incident had an intimidatory and silencing effect upon, and significant ramifications for, not only the affected individuals in terms of their reputation, wellbeing, safety and employment, but also the wider Jewish community, in terms of vilification and social exclusion. The incident thus highlighted the lack of adequate protections in the Act or in the Privacy Act[13] for vulnerable groups. This is despite the eSafety Commissioner having recognised that the harm caused by doxing can extend well beyond an affected individual.[14]

This gap in the Act should be addressed by the introduction of a separate section of the Act that recognises harms impacting protected groups. There may be instances where individuals – whether they are children or adults – may not wish to report a doxing incident or may not be able to demonstrate that the incident has met the requirements of sections 6 or 7 respectively, but it may

[12] 'Doxxing to be criminalised in Australia after Jewish Group Chat Leak', *Vice*, 13 February 2024: https://www.vice.com/en/article/dy3jjw/doxxing-australia-law-criminalised.
[13] *Privacy Act 1988 (Cth)*, registered 23 May 2024: Federal Register of Legislation - Privacy Act 1988
[14] The esafety Commissioner notes on its website that "on a broader level, using doxing as a form of digital vigilantism can have a negative impact on society through increasing lawlessness, conflict and reducing trust in public figures." See esafety Commissioner, 'Doxing: what is doxing or doxxing', 18 March 2024, https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing.

nevertheless be in the best interests of the vulnerable community to have its representatives seek to have the content taken down.

- **Non-consensual sharing of intimate images**

In Judaism, the body is the repository of the soul, and its rape, torture or mutilation is not just a crime, but also an offence against the Creator.[15] The sharing of non-consensual intimate images on online services, including images of deceased Jewish people, should give rise to the right for trusted representative bodies of the Jewish community such as the ECAJ to seek to have the image/s taken down. Such images may, in particular cases, glorify the rape, torture or mutilation of Jews as a group, celebrate the desecration of the Jewish soul, and incite violence against Jews more generally.

Recommendation 2: That a separate section of the Act be introduced to address group harms online, and to allow the eSafety Commissioner to accept reports of harmful content directed at protected groups if the reports are made by their trusted representative organisations. This will apply whether the content poses a risk to the safety of any individual or a protected group.

- **The Online Content Scheme**

The potential for harm to be inflicted on users online is very significant given the relative lack of regulatory oversight. The Act is built upon an expectation that industry do more to keep its users safe, including by developing mandatory, enforceable industry codes designed to protect Australians from illegal and restricted online content (Online Content Scheme). If a code does not meet statutory requirements under the Act, the Commissioner can develop an industry standard for that section of the online industry instead. However, it is not in industries' interests to develop extremely robust codes that impose additional costs on providers, nor would these codes be likely to address online harm directed at protected groups of people if there is less regulation in this area online.

The ECAJ proposes a different approach that is better aligned with contemporary models such as that adopted by the UK, whereby the regulator is responsible for drafting codes in consultation with industry. This would mitigate against the risk that industry codes are set by the most powerful and well-resourced organisations in any industry. However, in addition to the requirement for consultation with industry, we would add a requirement for consultation with representative bodies or associations of communities whose members engage with, or may be impacted by, online content produced by that industry.

This would help to address the chasm between the basic object of the Online Safety Act – to protect members of the Australian public from abusive conduct and harmful content online - and its current focus on representative industry bodies or associations. As the peak elected representative body of the Australian Jewish community, there should be a place for the ECAJ and other organisations like it which demonstrably represent various communities, to shape appropriate community safeguards. Representative bodies of communities, as well as of special interest

[15] See Sifrei Cohen to Leviticus 19:28; Rashi to Deuteronomy 14:1; Responsa Tzitz Eliezer 11:41.

groups, have a wealth of knowledge about how those whom they represent engage with online content and what the impacts are to their members.

To give but one example, in the event that the security or defence industries developed an electronic service which brought them within the ambit of one of the eight key sections of the online industry, and as such were giving input into an industry code with respect to Class 1 material, including pro-terror material and extreme crime and violence material, it would be appropriate for protected minority groups who suffer from specific security threats on the basis of their race or religion, to have the opportunity to provide feedback on a proposed code insofar as it related to the security or defence industry. This input from those who represent users of online content rather than just those who generate and host it, would result in codes that are more robust, practical and more aligned with the objects of the legislation.

Creating a mechanism in the Online Safety Act for trusted representative organisations of sections of the Australian public, and particularly protected groups, to engage with industries and with the eSafety Commissioner, would also increase the likelihood that obvious harm would be removed by platforms more expeditiously.

At present, protected groups and their representative bodies need to fund independent researchers to make artificial intelligence agents that monitor and record harmful content. The technology companies are far better-resourced and more capable of doing that work and using it to remove that harmful content quickly, especially where they know who to engage with, in order to get a view as to whether such content is indeed harmful. Some technology companies are already investing human and AI resources into doing this work to some extent, but the evidence is that self-regulation seems to come off second best if and when it conflicts with self-interest.

In addition, standards for both the response time and accuracy of responses by technology platforms, in answer to user reports of harmful content are needed. To be meaningful, there must be a way to test compliance, and significant penalties for persistent or systemic failure.

We would also propose that the reach and risk of platforms is part of the consideration for how tightly they are regulated. For example, while the reach of social media platforms such as Facebook, Twitter and Instagram is large, they have been ranked as lower risk entry platforms for extremist content than platforms such as 4chan, 8chan/Kun, Gab, Reddit and some others. This is because as individuals move from the larger platforms to the smaller online communities with less access to different opinions, confirmation bias is amplified.[16] A nuanced approach must be adopted in evaluating online harm, as higher reach platforms can serve to make online hatred towards protected groups more socially acceptable, and to funnel users to lower reach platforms that may incite violence.

Recommendation 3: That in the place of the current Online Content Scheme, the regulator be responsible for drafting codes in consultation with industry and trusted representatives of the Australian public including peak representative bodies of protected groups.

[16] See the submission of the Centre for Resilient and Inclusive Societies (CRIS) to the Senate Legal and Constitutional Affairs References Committee, April 2024: https://wordpress-ms.deakin.edu.au/adi/wp-content/uploads/sites/316/2024/04/CRIS-Submission-Senate-Inquiry-into-Right-Wing-Extremist-Movements-FINAL-V2.pdf

Recommendation 4: That additional regulatory requirements be introduced in respect of online services with higher risk and reach, using the UK risk-based regulatory regime as a model.

- **Material that depicts abhorrent violent conduct**

The ECAJ supports the continued existence of a mechanism for the eSafety Commissioner to request or require the blocking of material that promotes, incites, instructs in or depicts abhorrent violent conduct if the material is likely to cause significant harm to the Australian community. However, as mentioned in Section 1 of this submission, the Jewish community and other protected groups who regularly face online commentary denying the occurrence of historical and more recent atrocities are now in the difficult position where it is easier for online users to deny that abhorrent violent conduct took place than it is for the victims to publish the proof of that conduct. This means that an online culture of denial of abhorrent violent conduct is flourishing and extremist groups are able to build strong narratives that cannot be countered with visual proof by affected individuals or communities.

The debate about which online content was permissible in relation to the April 2024 Sydney stabbing attack on bishop Mar Mari Emmanuel highlights some of the difficulties in the current regulatory approach. The eSafety Commissioner sought to have a take-down notice enforced against X (formerly Twitter), which refused to remove the live-stream of the stabbing attack from its global platform but ultimately conceded to geo-blocking it[17] so that Australian users cannot access it without using a VPN. While the ECAJ fully supports the eSafety Commissioner's rationale in seeking to have the content removed, there is now space for online denial as to whether the stabbing of the bishop was a terrorist incident[18] and whether the incident even occurred.

The same can be said regarding the mass atrocities perpetrated by Hamas in Israel on 7 October 2023. This is because the live-streams videoed by the Hamas perpetrators of their atrocities have not been permitted to be aired in full online and individuals and organisations continue to deny that the massacre and associated atrocities such as systematic rape, mutilation and torture took place.[19] The ECAJ seeks a more holistic approach to material that depicts abhorrent violent conduct that would also remove content denying that the incident took place or content urging or endorsing the violence.

---

[17] 'Australia abandons legal battle to have graphic footage of Sydney church stabbing removed from X', *MSN.COM*, 5 June 2024: https://www.msn.com/en-us/news/world/australia-abandons-legal-battle-to-have-graphic-footage-of-sydney-church-stabbing-removed-from-x/ar-BB1nF5Er

[18] 'Another Sydney Stabbing', *Crikey*, 16 April 2024: https://www.crikey.com.au/2024/04/16/assyrian-church-teen-stabbing-bruce-lehrmann-defamation-fail-annual-leave/

[1919] See for example, Godsell, Oscar, 'Sydney University professor claims Hamas rape of women and baby beheadings "fake news" in student lecture', *Sky News Australia,* 31 May 2024: https://www.skynews.com.au/australia-news/sydney-university-professor-claims-hamas-rape-of-women-and-baby-beheadings-fake-news-in-student-lecture/news-story/f422cd8f7d06c63183fca2a16dd9563c; and 'Denialism in the wake of the Oct. 7 massacre', ADL, 19 December 2023: https://www.adl.org/resources/blog/denialism-wake-oct-7-massacre#:~:text=Since%20Oct.%207%2C%20many%20anti-Israel%20and%20antisemitic%20voices,was%20the%20one%20largely%20responsible%20for%20the%20massacre.

Recommendation 5: That the current regulatory regime with respect to material that depicts abhorrent violent conduct be enhanced by the adoption of appropriate vetting systems by service providers, at their cost, to ensure that content denying the carrying out of the abhorrent violent conduct in question is also removed and reported to the eSafety Commissioner.

3. The operation and effectiveness of the Basic Online Safety Expectations (BOSE) regime in the Act.

The Basic Online Safety Expectations (BOSE) do not impose a legally enforceable duty on service providers to implement the expectations, and they are broad and relatively abstract. Although the Commissioner may require service providers to report against the expectations contained in the BOSE Determination, there is a real question as to whether the Commissioner would be in a position to identify whether a provider had implemented the core and additional expectations adequately through the introduction of appropriate mechanisms.

The reporting requirement seems to be a reactive means of reviewing whether service providers are complying with the BOSE. It is likely that the only service providers who would come under scrutiny this way would be those who have attracted the attention of sophisticated users with the wherewithal and resources to engage with the Commissioner.

The ECAJ proposes a mandatory reporting system in which all service providers are required to report against the expectations outlined in the BOSE Determination, and to provide to the Commissioner a list of every site they have removed, along with the reason why, as well as the date of the complaint (if applicable) and the date of the removal. The ECAJ also recommends that service providers review and respond to complaints within a reasonable period of time, provide feedback to users on the actions taken[20], and provide the Commissioner with a report of all complaints including the date they were made, the basis for the complaint, and the outcome. We would propose that penalties are introduced for any repeated failure to meet the BOSE, and that the scope of the BOSE ought to extend to unlawful or harmful content that impacts a protected group.

Recommendation 6:
That:

- **a mandatory reporting system be introduced in which all service providers are required to report against the expectations outlined in the BOSE Determination;**
- **service providers be required to review and respond to complaints within a reasonable period of time, provide feedback to users on the actions taken, and provide the Commissioner with a report of all complaints including the date they were made, the basis for the complaint, and the outcome;**
- **the Commissioner be empowered, in the event of a repeated failure of a service provider to remove non-BOSE-compliant content, to order the immediate removal of the content.**

[20] The public consultation on a range of amendments to the Basic Online Safety Expectations Determination commenced in November 2023 and closed on 16 February 2024, and these were among the recommendations suggested by parties who made submissions.

- **these proposed reforms be extended to cover online harms impacting protected groups.**

4. **Whether additional arrangements are warranted to address online harms not explicitly captured under the existing statutory schemes, including:**
    a. **online hate**
    b. **volumetric (pile-on) attacks**
    c. **technology-facilitated abuse and technology-facilitated gender-based violence**
    d. **online abuse of public figures and those requiring an online presence as part of their employment**

a) Online hate

The eSafety Commissioner needs to be empowered to facilitate the interim removal of content that may be unlawful under any other Commonwealth, State or Territory law. This would ensure online/offline conformity via a general power to require interim removal of online content considered by another government agency to be prima facie harmful enough to be unlawful. At present, no mechanism exists for the Commissioner to be able to act on referral for breaches of Federal, State or Territory law in online spaces. Such a referral mechanism would assist the eSafety Commissioner in acting expeditiously to combat online hate and would provide the office of the Commissioner with an interim assessment from the relevant body tasked with oversight of the applicable legislation.

This would help ameliorate the risk of time delay in removal of unlawful hate speech online, as inadequate and tardy responses can have catastrophic consequences in this area. Insufficient attention to preventing hate speech online has allowed Australians access to radicalisation material. In at least the case of one Australian, this led to extremist indoctrination and behaviour with deadly results - as we saw in Christchurch in 2019. However, the kind of action that was taken against the Christchurch terrorist's manifesto (referral to the classification board) was not taken against the online terrorist manifesto from a terrorist attack that took place 7 months later (in Halle, Germany) despite being required by legislation. This inhibited efforts to get appropriate and timely action from Google, which in turn led to Australian taxpayers, and state governments, spending money on advertising that appeared alongside the terrorist manifesto and profited the person keeping it online.

After Christchurch, a protocol was developed with the Communications Alliance to deal with any future 'online crisis event', but this only deals with the problem after the event, and does not address inaction in the face of warning indicators leading to such an event.[21] In February 2024, the Standing Council of Attorneys-General acknowledged the rise in instances of vilification, especially online across social media platforms. The Council also articulated the Government's commitment to reforming the law to boost protections against vilification and hate speech.[22]

[21] See the ECAJ's letter to the eSafety Commissioner dated 16 February 2024.
[22] Standing Council of Attorneys-General Communiqué, 23 February 2024: https://www.ag.gov.au/sites/default/files/2024-02/scag-communique-february-2024.pdf.

By setting up a referral mechanism that empowers the eSafety Commissioner to facilitate the interim removal of content that is prima facie unlawful under any other Commonwealth, State or Territory law, the eSafety Commissioner will be better equipped to respond in a timely way to online instances of vilification and hate speech. There will also be an improvement in cross-government coordination on the regulation of online harms.[23]

By way of example, we outline here how the proposed referral mechanism would work with respect to online content that a complainant alleges has breached the Racial Discrimination Act 1975 (Cth) and which may have also breached the Online Safety Act 2021 (Cth). Complaints about breaches of the Racial Discrimination Act are pursued with the Australian Human Rights Commission (AHRC) whose President appoints an officer to investigate the complaint and attempt to resolve it by conciliation, failing which the matter can be taken to the Federal Court.[24] Complaints can be made about the doing or saying of anything *otherwise than in private* that is reasonably likely to cause offence, insult, humiliate or intimidate a person or group because of their race, colour, or national or ethnic origin. The publication of such material online, so that it is generally accessible to users, is *prima facie* unlawful.[25]

The ECAJ contends that in such instances, the President of the AHRC or the President's nominee, ought to be empowered to:

a. notify the eSafety Commissioner that the Commission has received a complaint under the AHRC Act that relates to online content; and
b. issue a temporary take down notice until the complaint before the AHRC or any consequent legal proceedings have been concluded.

Under this proposed mechanism, there are other agencies that would be able to make a referral to the eSafety Commissioner for alleged online breaches of Federal, State or Territory law, depending on the nature of the alleged online conduct. There may also be instances where expert bodies are empowered to make a referral, including the independent expert bodies under international treaties that Australia has ratified, such as the Committee on the Rights of the Child as per the Convention on the Rights of the Child. This online and offline conformity is necessary and should be approached in a way that is not unduly prescriptive, given that new pieces of legislation will enter into force from time to time which will require a harmonised offline and online response.

(b) Volumetric (pile-on) attacks

Representative bodies and prominent leaders in the Jewish community are easy targets for volumetric (pile-on) attacks. Almost every time the ECAJ's co-CEO Alex Ryvchin publishes a post on any social media platform he is targeted with volumetric attacks that intensify in their level of outrage or toxicity and at times appear to be coordinated. Often these online attacks are followed with the receipt of hate mail, demonstrating the real connection between online hate and offline antisemitic incidents.

---

[23] This is the second priority outlined by the Australian Government in its response to the House of Representatives Select Committee on Social Media and Online Safety report: 20230330 - Australian Government response to the Social Media and Online Safety inquiry (infrastructure.gov.au), pp. 3.
[24] Section 46PO of the *Australian Human Rights Commission Act* 1986 (Cth)
[25] *Jones v Toben* (includes explanatory memorandum) [2002] FCA 1150, paras 71-75 *per* Branson, J.

In such pile-on attacks, the Act's requirement that each individual post be assessed against the threshold for regulatory action under the child cyberbullying or adult cyber-abuse schemes is not appropriate because the harm is inflicted cumulatively, and it is also the case that prominent community representatives may not wish to show vulnerability by complaining about individual posts. There is also a very real security threat posed by these volumetric attacks, and affected individuals from protected groups may be reluctant to take action against specific individuals. It is for this reason that many of the Jewish or Israeli targets of posts by social media influencers have avoided making a complaint. Each individual post may not be sufficient to warrant regulatory action, but some influencers have followings that are so large that once they post an attack against an individual, it is sure to be followed by attacks from their followers, and where the subject fights back the pile-on intensifies.

(c) Technology-facilitated abuse and technology-facilitated gender-based violence

The ECAJ's recommendations with respect to addressing online harms impacting groups are also relevant in this area given that surveys have established the link between technology-facilitated abuse and vulnerable groups.[26]

(d) Online abuse of public figures and those requiring an online presence as part of their employment

The Online Safety Act contains a gap with respect to defamation and racial vilification in that it requires the abuse to be "seriously harmful" before the eSafety Commissioner can act on a report of cyber-abuse of an adult. This may be a higher threshold in some instances than is required in:

- defamation law - which is focused on harm caused to an individual's reputation; or
- Section 18C of the Racial Discrimination Act 1975 (Cth), which makes it unlawful for someone to do an act that is reasonably likely to "offend, insult, humiliate or intimidate" someone because of their race or ethnicity.

While this discrepancy is explicable in the sense that the Act aims to minimise physical and psychological harm to targets of cyber abuse, one can envisage many situations where defaming or racially vilifying a prominent member of a minority community results in a heightened sense of threat and insecurity among members of that community as a whole, and exacerbates or creates a threat, even if it cannot be said that the risk of harm to that particular individual increases.

One can also envisage a situation where a public figure requiring an online presence as part of their employment would be able to establish that the online abuse in question is "seriously harmful", but they are not minded to make a report to the eSafety Commissioner, possibly because they are desensitized to such abuse, do not have the resources (including the time) required to take action, wish to avoid appearing vulnerable, or many other factors.

In either of these instances, representatives of the community or the community organisation whom the public figure is associated with ought to be able to seek removal of the online content in question on the basis that it has a seriously harmful silencing effect or an adverse impact on the

[26] See Australian National Research Organisation for Women's Safety (ANROWS), Technology-facilitated abuse: National survey of Australian adults' experiences, July 2022, 8, 4AP.3-Flynn-TFa3-Survey-of-VS.pdf (anrowsdev.wpenginepowered.com), accessed 26 April 2024.

sense of safety or security on the community as a whole. For instance, we attach at Appendix 1 an example of online abuse of public figures of the Jewish community in the lead-up to the Voice Referendum in October 2023. While the online abuse was antisemitic and may have been deemed to breach state, territory or Commonwealth laws had the community leaders in question sought to make a legal complaint, the abuse also had a threatening and chilling impact on the Jewish community as a whole. Such abuse had the effect of discouraging members of the Jewish community from campaigning in support of the Voice or publicising their support for the Voice on online platforms, because they would have been aware of the abuse that community leaders experienced.

Recommendation 7: That additional arrangements are introduced to address online harms not explicitly captured under the existing statutory schemes, including online hate, volumetric (pile-on) attacks, technology-facilitated abuse and online abuse of public figures and those requiring an online presence as part of their employment.

These additional arrangements should include:

- **setting up a referral mechanism that empowers the eSafety Commissioner to facilitate the interim removal of content that may be unlawful under any other Commonwealth, State or Territory law, following a referral from another government agency that considers the content to be prima facie harmful enough to be unlawful.**
- **assessing volumetric (pile-on) attacks for their cumulative impact rather than assessing each individual post. Where the volumetric attack is aimed at harming a protected group rather than an individual there should be scope for the eSafety Commissioner to take down the content under a separate section of the Act that:**
    - **addresses group harms, and**
    - **empowers trusted mainstream representative bodies of protected groups to seek to have such content taken down**
- **creating a mechanism whereby representative organisations on behalf of an individual/public figure, or the individual/public figure themselves may seek removal of online content on the basis that it has a seriously harmful silencing effect on a protected group as a whole.**

(e) Other potential online safety harms raised by a range of emerging technologies, including but not limited to:

i. generative artificial intelligence
ii. immersive technologies
iii. recommender systems
iv. end-to-end encryption
v. changes to technology models such as decentralised platforms

There is currently a consultation underway on a range of amendments to the Basic Online Safety Expectations Determination which will consider key proposed reforms including in the areas outlined in 4(c) above. The ECAJ did not make a submission to that consultation as it goes beyond the scope of our direct expertise and objects. Nevertheless, as outlined in Section 3 above, we would urge that the breadth of the Basic Online Safety Expectations be widened to encompass unlawful or harmful content that impacts a protected group. These emerging technologies do offer

the potential for additional online safety, but they also carry risks, for example recommender systems may further embed confirmation bias – an obvious threat with regard to antisemitic discourse. End-to-end encryption may offer enhanced security for communications, but it will also make investigation of extremist groups more challenging for law enforcement. Generative artificial intelligence has the potential to amplify online harms by creating synthetic material that has no semblance to truth. A policy paper released by the United Nations Educational, Scientific and Cultural Organisation with the World Jewish Congress found that AI technology is helping to create false stories about World War II atrocities including Holocaust denial, risking an "explosive spread of antisemitism".[27] The document highlights instances where hackers rigged chatbots to spread Nazi ideology, and others where bots dreamed up their own stories around the Holocaust. This has clear implications for online and offline antisemitism. The risks posed to protected groups by this technology necessitate a widening of the BOSE.

Recommendation 8: That the Act remain technology-neutral and retain its focus on online harms rather than the way such harms are inflicted.

Recommendation 9: That the breadth of the Basic Online Safety Expectations be widened to encompass unlawful or harmful content that impacts a protected group.

5. **Whether the regulatory arrangements, tools and powers available to the Commissioner should be amended and/or simplified, including through consideration of:**
    a. **the introduction of a duty of care requirement towards users (similar to the United Kingdom's Online Safety Act 2023 or the primary duty of care under Australia's work health and safety legislation) and how this may interact with existing elements of the Act**

The hybrid approach to online safety adopted in Australia offers individuals the opportunity to complain about types of harmful content as well as encouraging platforms to promote systems and processes. It is the ECAJ's view that it would nevertheless be bolstered by the introduction of stronger duties on service providers.

The introduction of a duty of care requirement towards users that is similar to that which is provided for in the United Kingdom's Online Safety Act 2023 and places duties on the entities which control the regulated environment would seem to be an improvement upon Australia's current framework. Such an approach would place those entities that are closest to fast-paced changes in the online environment, and which stand to gain the most from those, in a position of responsibility for minimising harm that flows from their environments.[28] We believe this is necessary. Recent data from the Online Hate Prevention Institute shows that in the past 18 months alone, 5,008 items of antisemitism have been identified online, of which 4,372 were collected

[27] Makhortykh, Mykola [author], Mann, Heather [editor] 'AI and the Holocaust: rewriting history? The impact of artificial intelligence on understanding the Holocaust', UNESCO, 2024: https://unesdoc.unesco.org/ark:/48223/pf0000390211

[28] Carnegie UK 2022 Submission to the House Select Committee on Social Media and Online Safety, January 2022, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Submissions, pp. 12

since 7 October 2023.[29] As discussed above, recognising online harm to protected groups is an essential area of reform of the Act, but without a duty of care requirement and more onerous obligations on service providers it is unrealistic to think that service providers would proactively identify such content and remove it quickly.

The addition of a statutory duty of care would help transform the expectations in the BOSE into legally enforceable duties with penalties for non-compliance.

b. ensuring industry acts in the best interests of the child

This area goes beyond the scope of the ECAJ's mission, however, please refer to our recommendations in Section 2, including our comments in the section titled 'Cyber-bullying material targeted at an Australian child or at an Australian adult'.

Recommendation 10: That a statutory duty of care be introduced into Australia's existing hybrid model, which would extend beyond the current scope of the Act and would also cover online harms inflicted on protected groups.

6. Whether penalties should apply to a broader range of circumstances.

Newer online safety regimes such as those in the United Kingdom and European Union take a different approach to Australia with respect to the quantum and calculation of penalties. Their approach, which includes imposing penalties based on a percentage of an online platform's global revenue, would seem to be more effective, fair and in conformity with the ECAJ's proposal in Section 2 above that the reach and risk of platforms is factored into how tightly they are regulated.

Penalties under the Act at present are not sufficiently onerous to act as a deterrent to misconduct by large online service providers or particular individuals. The maximum penalty at present is $156,000 for individuals and $782,500 for corporations.[30] These amounts would be significant for some individuals and companies but would be inconsequential for the likes of Meta, X (formerly Twitter) or Tiktok. The current regulatory approach to penalties therefore lends itself to imposing the harshest punishment on the smallest service providers who are unlikely to have the reach to cause as much harm as their bigger counterparts.

The ECAJ also proposes that a sliding scale of penalties and offences is introduced within the Act such that the most serious offences, and those that are more systemic, are penalised more harshly. At present the Act imposes the same maximum civil penalties on offences that cause very different levels of harm. From a penalty perspective, the Act also fails to differentiate between systemic failures to comply and non-compliance in particular cases. With respect to group harms online, the potential for offline incitement and racial hatred against a group is significant, and as noted earlier there is data to demonstrate that such harms are now generated systemically.[31] The penalty scale ought to reflect that.

[29] This data has been provided directly by the Online Hate Prevention Institute but has not yet been published. It will be released in a report in coming months.
[30] Though there is the possibility of a civil penalty being applied for each day where a required action is not taken.
[31] For example, a policy paper released by the United Nations Educational, Scientific and Cultural Organisation with the World Jewish Congress has shown how AI technology is helping promote Holocaust denial across platforms:

Other powers should be vested in the Commissioner including the power to compel some types of provider to stop working with a non-compliant service provider in order to undermine the latter's income stream. (An example would be payment providers being compelled not to work with a persistently non-compliant internet search engine or social media service). At present the Commissioner may apply for a Federal Court order that a person stop providing a particular type of online service if the person has contravened a civil penalty provision in the Online Content Scheme two or more times in the previous twelve months and the continued operation of the service operation therefore represents a community safety risk. The ECAJ supports retaining that provision, but the assessment of whether there is a community safety risk should be expanded to include group harm.

Recommendation 11: That penalties under the Act be based on a calculation of the higher of a fixed percentage of annual global turnover or a fixed amount sufficient to deter platforms with large revenue streams and significant reach, against non-compliance.

Recommendation 12: That a sliding scale of penalties and offences be introduced so that the most serious offences, and those that are more systemic, are penalised more heavily.

Recommendation 13: That the Commissioner's power to take action against repeat offenders should be retained but should be extended so as to enable the imposition of penalties for online harms inflicted on protected groups.

7. Whether the current information gathering powers, investigative powers, enforcement powers, civil penalties or disclosure of information provisions should be amended.

In addition to Recommendation 6 in Section 3 above, the ECAJ would propose that providers that operate in Australia and to which the Act applies should be required to produce to the eSafety Commissioner, at their own cost, an annual eSafety report from an independent auditor (i) certifying that the company's standards, including its policy regarding response times to complaints, meets regulatory requirements and (ii) reporting on the company's level of compliance with its own standards. As part of the process, the auditor should be required to advertise the audit beforehand and invite public submissions. The reports should be freely accessible by members of the public.[32] This would complement the reforms suggested above with respect to reporting against expectations outlined in the BOSE Determination.[33]

The ECAJ would also suggest that providers to which the Act applies are required to gather adequate user information such that the Commissioner is not hamstrung at a future date when exercising their power to obtain identity information regarding an end-user of a social media service, relevant electronic service, or designated internet service in circumstances contemplated by the Act[34]. While there are good reasons why users may seek to be anonymous on various online

---

Makhortykh, Mykola [author], Mann, Heather [editor] 'AI and the Holocaust: rewriting history? The impact of artificial intelligence on understanding the Holocaust', UNESCO, 2024: https://unesdoc.unesco.org/ark:/48223/pf0000390211

[32] See the ECAJ's letter to the eSafety Commissioner dated 16 February 2024.

[33] This is a similar approach to that adopted in the European Union.

[34] This power is contained in Section 194 of the Online Safety Act: C2022C00052.pdf

services, the service provider should be able to securely store basic identity information without it becoming publicly accessible – in compliance with privacy legislation - so that the online environment does not become one where individuals or organisations can commit unlawful acts without consequence. This requirement could be underpinned by the annual esafety report, in which the auditor would also attest to the provider having collated adequate identifying information for all users. This is analogous to the position under anti-money laundering legislation, where financial institutions and regulated entities are required to verify customers' identities and activities.[35] Such reporting obligations also have parallels in other legislation such as the Modern Slavery Act 2018 (Cth). In the event that the eSafety Commissioner exercises the power to obtain identity information of an end-user of a social media service, relevant electronic service, or designated internet service, and the service is unable to provide adequate data, then a penalty should apply.

The European and UK approaches offer some additional protections for online safety by providing the regulator with the power to compel access for accredited researchers to data from very large online platforms and search engines. This approach may be necessary, for example, when the Commissioner is assessing whether to exercise online safety functions.

There is a strong need for additional online safety support for the public, community organisations, and increasingly local government. Expert civil society organisations, including Online Hate Prevention Institute (OHPI), are able to provide support, but funding from the industry and government needs to be made available for this.[36]

Recommendation 14: That providers that operate in Australia and to which the Act applies be required to produce to the eSafety Commissioner, at their own cost, an annual eSafety report from an independent auditor. Such providers must also make representations in the report that they can verify the identities of their users.

8. **The Commissioner's functions and governance arrangements, including:**
    a. **the Commissioner's roles and responsibilities under the Act**
    b. **whether the current functions and powers in the Act are sufficient to allow the Commissioner to carry out their mandate.**

As noted throughout this submission, the ECAJ's view is that the Commissioner's powers are currently insufficient to meet the range of challenges to online safety that currently exist, and that reform is needed in this area. Enhanced functions and powers would better enable the Commissioner to identify and take action against a proposed new category of online harm directed at protected groups and would enable the Commissioner to discharge her roles and responsibilities under the Act more effectively. To that end, the ECAJ has made several recommendations throughout this submission as to how to enlarge the Commissioner's roles and responsibilities and equip the Commissioner with adequate powers to deliver on an enlarged remit.

[35] 'A Guide to KYC Requirements in Australia', Global Data, 19 April 2024: A Guide to KYC Requirements in Australia (globaldata.net.au).
[36] See the ECAJ's letter to the eSafety Commissioner dated 16 February 2024.

9. **Whether the current governance structure and support arrangements for the Commissioner provided by the ACMA are fit for purpose for both the Commissioner and the ACMA.**

It is ECAJ's view that the current governance structure of the Commissioner – as an independent statutory office with staff and support provided by the ACMA – is broadly appropriate, but that there needs to be scope for the Commissioner to seek outside expertise where it is necessary to inform decision-making.

For instance, the Act stipulates that the Commissioner may obtain advice from the Classification Board in relation to a range of areas including Class 1 and Class 2 Material.[37] However, one can envisage many situations where it would assist the Commissioner to seek advice from other experts or bodies. The Classification Board is established by the Classification (Publications, Films and Computer Games) Act 1995 and is comprised of individuals who have expertise in communications and the Arts. This structure does not seem like an ideal fit for assessing Class 1 and Class 2 Material, which may benefit from the expertise of those with a broader range of expertise and experience in counter-terrorism, law enforcement, criminal law, or in addressing other forms of anti-social behaviour that manifests online. The ECAJ notes that juxtaposing the National Classification Scheme and National Classification Code onto online content does not necessarily help address some of the more significant harms in the online arena, particularly with respect to group harms. The ECAJ would instead suggest that the Commissioner should be able to obtain advice from the relevant law enforcement agencies or agencies tasked with oversight of legislation in the relevant area to which the harm relates.

As with any reform, the structure will need to be much better resourced to meet the challenges posed by online safety (See response to Term 10 below).

Recommendation 15: That the Commissioner be empowered to seek and obtain input beyond the Classification Board where appropriate, and that the Commissioner be better resourced to engage in more in-depth exploration of harms associated with restricted and illegal online content, and solutions to address those.

10. **Whether it would be appropriate to cost recover from industry for eSafety's regulatory activities.**

It is the ECAJ's view that it is appropriate for the Government to recover from industry the costs of eSafety's regulatory activities. Industry benefits financially from providing online services, and the cost of regulating such services is a cost of doing business. This approach would be consistent with that taken in jurisdictions such as the UK and the EU, where cost recovery exists in certain circumstances. It is beyond the scope of the ECAJ's expertise and objects to advise on the best cost recovery models, but we endorse the principle and believe that it will improve online safety for users.

The Australian government should also increase its Budget allocation for eSafety given the challenges and opportunities that exist in this realm. The online environment is a global one and better coordination is required between the Department of Foreign Affairs and Trade, eSafety, the

[37] See Sections 106, 107 and 160, Online Safety Act, 2021 (Cth): C2022C00052.pdf

Australian Human Rights Commission, the Australian Federal Police, and relevant Australian civil society actors. The Australian government needs to facilitate and fund this international engagement either directly or via an impost on technology companies, including both the costs and time of civil society experts.

Recommendation 16: That the eSafety Commissioner be empowered to recover the costs of its regulatory activities from providers, including in the proposed new areas put forward in this submission.

Conclusion

We thank you for the opportunity to put our views forward, together with our recommendations aimed at improving the online safety of individuals and communities.

Yours sincerely

Peter Wertheim AM
Co-CEO

Simone Abel
Head of Legal

[Appendices follow on next page]

Appendix 1

Twitter posts reported to e-Safety Commissioner

Reported to e-commissioner 12 July 2023:

https://twitter.com/databased_01/status/1678489508029820928

https://twitter.com/databased_01/status/1678489431802540036

https://twitter.com/databased_01/status/1678489377666658338

https://twitter.com/databased_01/status/1678487466192302088

https://twitter.com/databased_01/status/1678489918283083788

https://twitter.com/auseconomicunit/status/1675383659166040065

https://twitter.com/cobcel1788/status/1674680770118680578

https://twitter.com/cobcel1788/status/1674677774097993729

https://twitter.com/cobcel1788/status/1672199489443213312

The content includes images of the PM and of prominent Jews. The content vilifies and defames the Jewish community by accusing them of being behind the Voice.

Office of the eSafety Commissioner

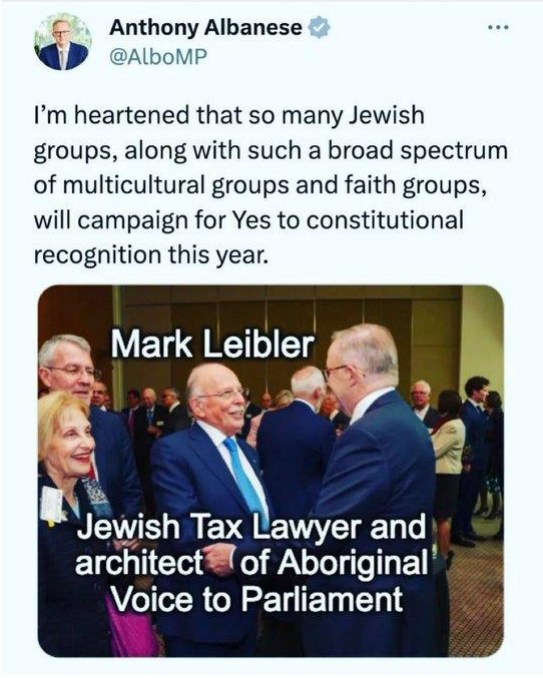
Your reference number is: **CYR-0201835**

…

Reported

https://twitter.com/databased_01/status/1678489508029820928

speakfreely@databased_01



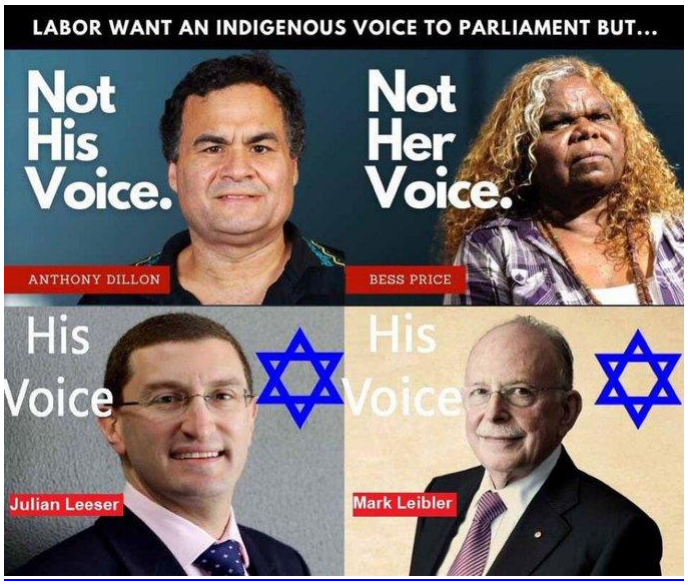
5:40 AM · Jul 11, 2023
·**13**Views

…

Reported

https://twitter.com/databased_01/status/1678489431802540036

speakfreely@databased_01



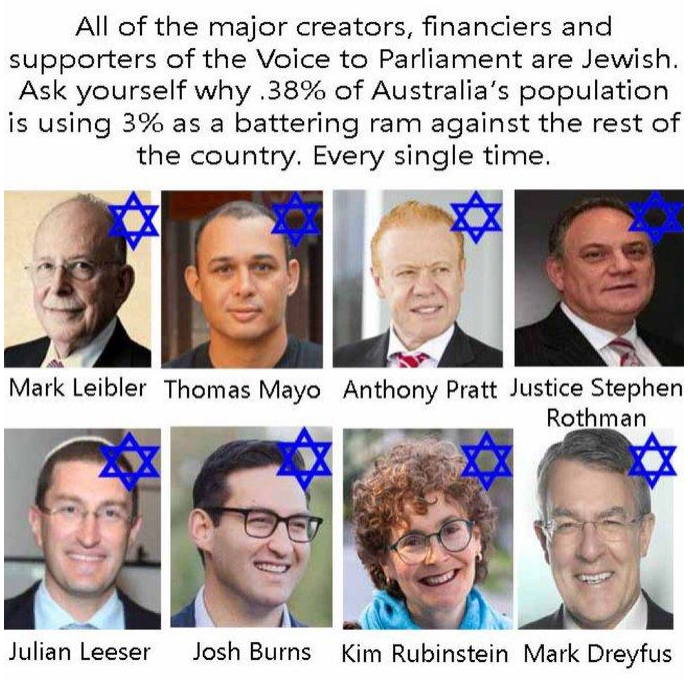
[5:40 AM · Jul 11, 2023]
·**12**Views

…

Reported

https://twitter.com/databased_01/status/1678489377666658338

speakfreely@databased_01

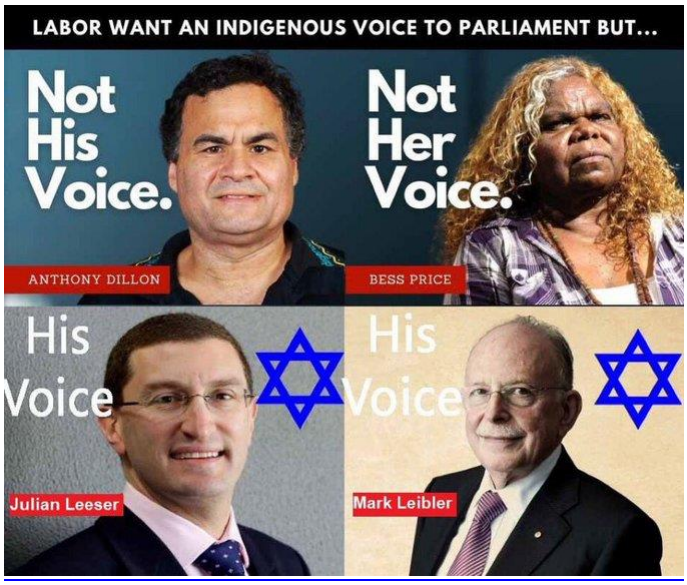


5:40 AM · Jul 11, 2023
·
13 Views

…

Reported
https://twitter.com/databased_01/status/1678487466192302088

speakfreely@databased_01
The goyim know

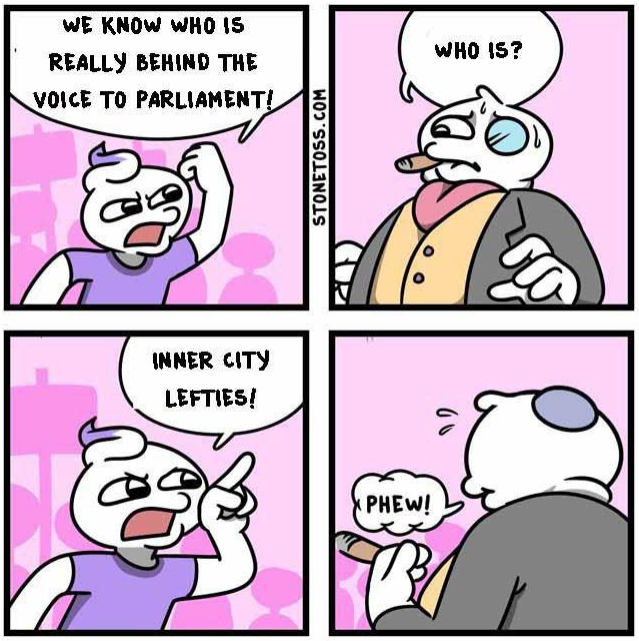


5:32 AM · Jul 11, 2023
·**114**Views

…

https://twitter.com/databased_01/status/1678489918283083788

speakfreely@databased_01

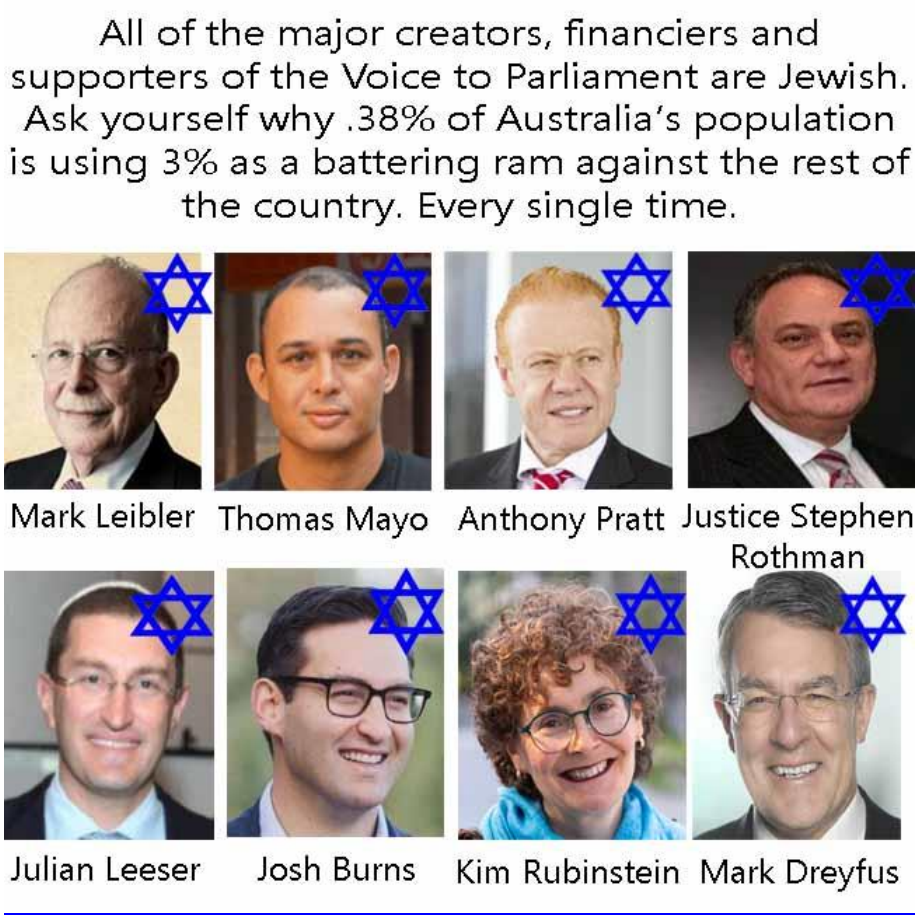


5:42 AM · Jul 11, 2023
·
10 Views

...

reported
https://twitter.com/auseconomicunit/status/1675383659166040065

EZFKA@auseconomicunit
Just a totally organic cohencidence for the betterment of Australia and totally not the latest chapter in the thousands year old hate and attempted destruction of white people. cc:
@OJhitler

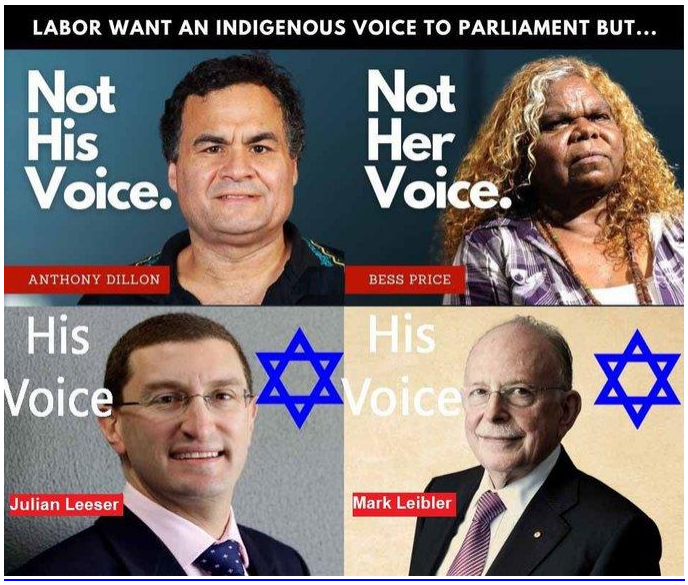


3:59 PM · Jul 2, 2023
·
4,785 Views

…

https://twitter.com/cobcel1788/status/1674680770118680578

NJF36 @cobcel1788
The Jewish voice



5:26 PM · Jun 30, 2023
·
4,726 Views

…

Reported

https://twitter.com/cobcel1788/status/1674677774097993729

NJF36 @cobcel1788
and there it is... #VoteNo to the Jewish voice.
Quote Tweet

Anthony Albanese@AlboMP·Jun 30
I'm heartened that so many Jewish groups, along with such a broad spectrum of multicultural groups and faith groups, will campaign for Yes to constitutional recognition this year.

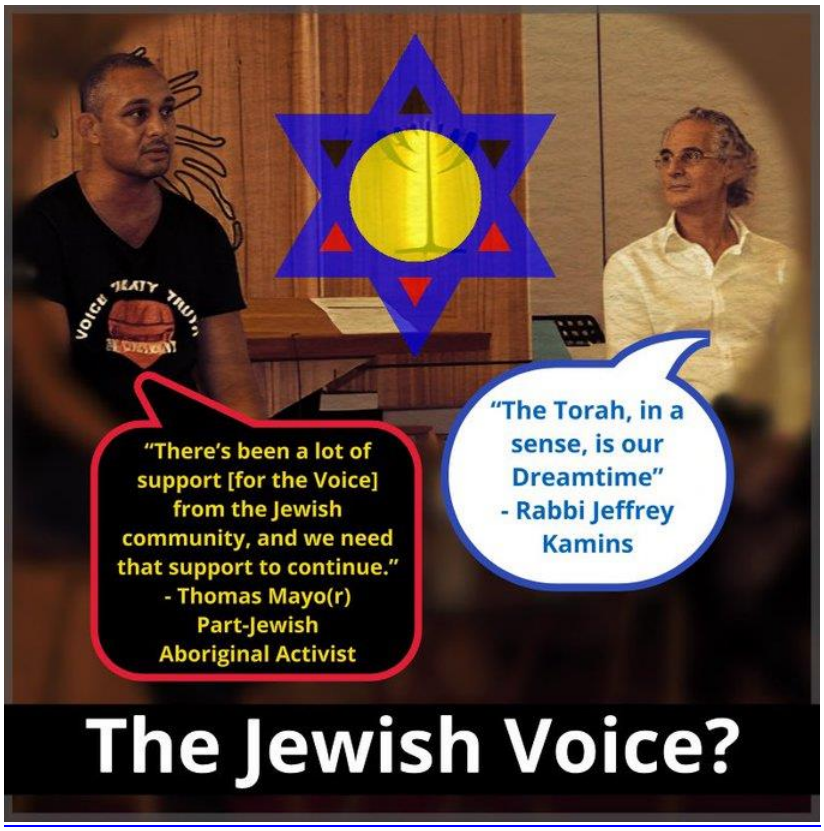
5:14 PM · Jun 30, 2023
·
296 Views

…

Reported

https://twitter.com/cobcel1788/status/1672199489443213312

NJF36 @cobcel1788
The Jewish Voice to Parliament



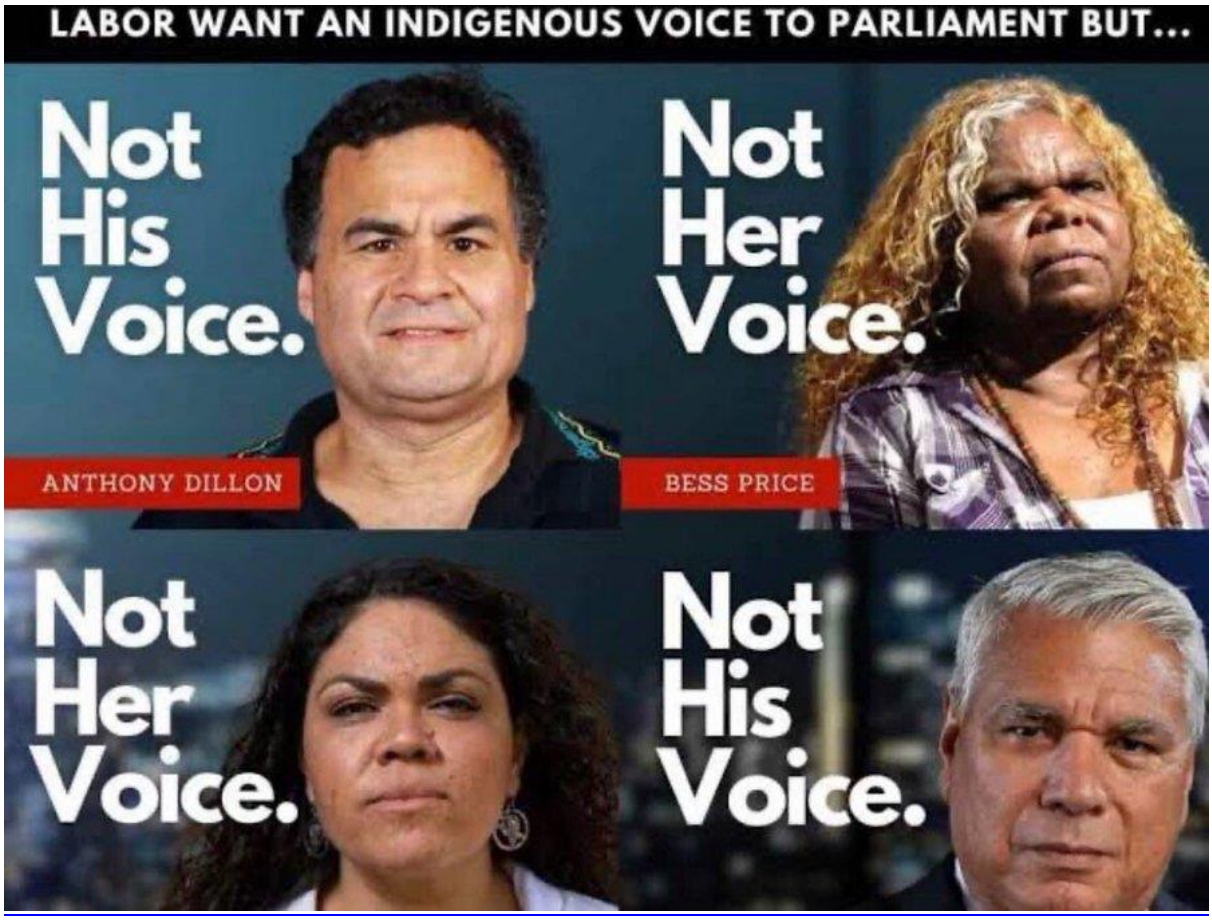
9:06 PM · Jun 23, 2023
·**341** Views

//

Shows alternate image

https://twitter.com/ShazbuzJames/status/1681115130564870145

Shazzie James@ShazbuzJames
#VoteNoToRacistVoice
@JNampijinpa
Jacinta Price has the biggest following on FB. No one comes close. Her words are wise and truth telling. Vote No to this racist voice.



11:34 AM · Jul 18, 2023
·
13.2K
Views

//

From: eSafety Hotline <online@esafety.gov.au>
Sent: 13 July 2023 16:04
To: [redacted]
Subject: Your complaint to the eSafety Commissioner - Reference CYR-0201835 [SEC=OFFICIAL:Sensitive] CRM:0103553

Dear Julie,

Thank you for your report to the eSafety Commissioner.

We can only direct online service providers to remove or age restrict access to online content if it class 1 or class 2 material. This includes material that shows child sexual abuse, terrorism, extreme violence and material not suitable for children.

Further information about illegal and restricted content is available from our website at: https://www.esafety.gov.au/key-issues/Illegal-restricted-content

Regards,
Illegal and Restricted Content Team
eSafety Commissioner
E online@esafety.gov.au
W www.esafety.gov.au

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Appendix 2

List of recommendations of the Executive Council of Australian Jewry to the statutory review of the Online Safety Act 2021

Recommendation 1: That the overarching objects in section 3 of the Act be amended so as to provide explicitly for the improvement and promotion of online safety for individuals *and protected groups*.

Recommendation 2: That a separate section of the Act be introduced to address group harms online, and to allow the eSafety Commissioner to accept reports of harmful content directed at protected groups if the reports are made by their trusted representative organisations. This will apply whether the content poses a risk to the safety of any individual or a protected group.

Recommendation 3: That in the place of the current Online Content Scheme, the regulator be responsible for drafting codes in consultation with industry and trusted representatives of the Australian public including peak representative bodies of protected groups.

Recommendation 4: That additional regulatory requirements be introduced in respect of online services with higher risk and reach, using the UK risk-based regulatory regime as a model.

Recommendation 5: That the current regulatory regime with respect to material that depicts abhorrent violent conduct be enhanced by the adoption of appropriate vetting systems by service providers, at their cost, to ensure that content denying the carrying out of the abhorrent violent conduct in question is also removed and reported to the eSafety Commissioner.

Recommendation 6:
That:

- a mandatory reporting system be introduced in which all service providers are required to report against the expectations outlined in the BOSE Determination;
- service providers be required to review and respond to complaints within a reasonable period of time, provide feedback to users on the actions taken, and provide the Commissioner with a report of all complaints including the date they were made, the basis for the complaint, and the outcome;
- the Commissioner be empowered, in the event of a repeated failure of a service provider to remove non-BOSE-compliant content, to order the immediate removal of the content.
- these proposed reforms be extended to cover online harms impacting protected groups.

Recommendation 7: That additional arrangements are introduced to address online harms not explicitly captured under the existing statutory schemes, including online hate, volumetric (pile-on) attacks, technology-facilitated abuse and online abuse of public figures and those requiring an online presence as part of their employment.

These additional arrangements should include:

- setting up a referral mechanism that empowers the eSafety Commissioner to facilitate the interim removal of content that may be unlawful under any other Commonwealth, State or Territory law, following a referral from another government agency that considers the content to be prima facie harmful enough to be unlawful.
- assessing volumetric (pile-on) attacks for their cumulative impact rather than assessing each individual post. Where the volumetric attack is aimed at harming a protected group rather than an individual there should be scope for the eSafety Commissioner to take down the content under a separate section of the Act that:
    - addresses group harms, and
    - empowers trusted mainstream representative bodies of protected groups to seek to have such content taken down
- creating a mechanism whereby representative organisations on behalf of an individual/public figure, or the individual/public figure themselves may seek removal of online content on the basis that it has a seriously harmful silencing effect on a protected group as a whole.

Recommendation 8: That the Act remain technology-neutral and retain its focus on online harms rather than the way such harms are inflicted.

Recommendation 9: That the breadth of the Basic Online Safety Expectations be widened to encompass unlawful or harmful content that impacts a protected group.

Recommendation 10: That a statutory duty of care be introduced into Australia's existing hybrid model, which would extend beyond the current scope of the Act and would also cover online harms inflicted on protected groups.

Recommendation 11: That penalties under the Act be based on a calculation of the higher of a fixed percentage of annual global turnover or a fixed amount sufficient to deter platforms with large revenue streams and significant reach, against non-compliance.

Recommendation 12: That a sliding scale of penalties and offences be introduced such that the most serious offences, and those that are more systemic, are penalised more heavily.

Recommendation 13: That the Commissioner's power to take action against repeat offenders should be retained but should be extended so as to enable the imposition of penalties for online harms inflicted on protected groups.

Recommendation 14: That providers that operate in Australia and to which the Act applies be required to produce to the eSafety Commissioner, at their own cost, an annual eSafety report from an independent auditor. Such providers must also make representations in the report that they can verify the identities of their users.

Recommendation 15: That the Commissioner be empowered to seek and obtain input beyond the Classification Board where appropriate, and that the Commissioner be better resourced to engage in more in-depth exploration of harms associated with restricted and illegal online content, and solutions to address those.

Recommendation 16: That the eSafety Commissioner be empowered to recover the costs of its regulatory activities from providers, including in the proposed new areas put forward in this submission.