Senate Legal and Constitutional Affairs Legislation Committee

Attorney-General's Department

Hearing date: 23 July 2024

Hansard page: 49

Paul Scarr asked the following question:

Senator SCARR: That's right. It's for everyone's enjoyment. I want to quote from Relationships Australia in their submission, page 16. This is in relation to an exception to the offence in paragraph 474.17A(1)(c) in relation to genuine medical or scientific purpose. This is what Relationships Australia say:

The proposed exception is regressive, in that it fails to reflect significant advances, over the past three decades, in medical jurisprudence concerning the autonomy, dignity and privacy rights of persons receiving health care. It is deeply surprising to find it in a Bill introduced into the Australian Parliament in 2024.

The proposed exception is contrary to the guidance produced by the Australian Medical Association and the Medical Indemnity Industry Association of Australia for medical students and doctors, Clinical images and the use of personal mobile devices. This guidance makes very clear the significance of consent in clinical photography, as does similar guidance provided by the Royal Australian College of General Practitioners.

I can perhaps give that to you on notice to have a look at, or you might have a response now. I'd be interested in your response in light of the guidance from the AMA and the Medical Indemnity Industry Association with respect to what is reasonable practice in a medical context in terms of taking extraordinarily private images and using them for other purposes in a medical context. On the face of it, it concerned me, that observation. Do you have any response now?

Mr Reeve: I will take that on notice. The one observation I would make at this point is perhaps the distinction between a breach of the Privacy Act or professional obligations to a patient that may attract professional sanctions or civil penalties under those frameworks, and the imposition of criminal liability under the Criminal Code, as to whether there is a justifiable distinction between the approach we would take in those two contexts.

The response to the question is as follows:

Civil and criminal law frameworks operate alongside but separately to professional standards and guidelines, and breaches of professional responsibilities need to considered in each of these separate contexts.

Professional standards and guidelines, such as the Australian Medical Association (AMA) and the Medical Indemnity Industry Association of Australia (MIIAA)'s guide: *Clinical images*

and the use of personal mobile devices,[1] are intended to be read in conjunction with any relevant legislation. The guide outlines key ethical and legal issues to be aware of before using a personal mobile device to take or transmit clinical images for the purposes of providing clinical care. It is a best practice manual that is intended to assist medical students and doctors in a clinical setting.[2] Obligations under relevant privacy laws still apply.

The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 targets the non-consensual sharing of sexually explicit material online, and has a maximum penalty of 7 years' imprisonment. The exceptions in the Bill are necessary to ensure that there are appropriate defences to criminal liability under the *Criminal Code* (Cth). The offence-specific defences in the Bill for the sharing of material for genuine scientific or medical purposes apply only in relation to the proposed new offences, and do not affect the operation of professional standards or guidelines, or privacy laws.

[1] https://ama.com.au/sites/default/files/documents/FINAL_AMA_Clinical_Images_Guide.pdf

[2] In addition, the Australian Health Practitioner Regulation Agency (AHPRA) has in place guidance for social media for all health practitioners: https://www.ahpra.gov.au/Resources/Social-media-guidance.aspx. All National Boards have in place a code of conduct which includes direction on privacy and ethical considerations: https://www.ahpra.gov.au/Resources/Code-of-conduct.aspx.

Senate Legal and Constitutional Affairs Legislation Committee

Attorney-General's Department

Hearing date: 23 July 2024

Hansard page: 49

Larissa Waters asked the following question:

Senator WATERS:..... To the constitutional barriers, I'd like to know whether the AGs have sought legal advice on whether you could use the external affairs power and our signatory status to CEDAW, the convention on discrimination against women, as a possible basis for an offence of creating this material—not the one that's proposed of creating and disseminating it, but just a creating offence. That seems to me to be within the scope of jurisdiction, so I'd like to know whether you've turned your minds to that and whether you had any legal advice saying that it was a goer or not.

The response to the question is as follows:

In drafting the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024, the Attorney-General's Department obtained legal advice from the Australian Government Solicitor on constitutional risk, including for a creation offence.

Senate Legal and Constitutional Affairs Legislation Committee

Attorney-General's Department

Hearing date: 23 July 2024

Hansard page: 49

Larissa Waters asked the following question:

Senator WATERS: ...I'd also like to know about funding for sexual violence services under the national plan and whether, in particular, there are enough specific things in the plan that funding for sexual violence services could be justified by to do prevention work around image-based abuse. The services say they've got the expertise to do that prevention work with perpetrators, and perhaps it's more for repeat offenders—but whether you think there's sufficient emphasis in the plan to justify that funding decision, should government choose to allocate funds in that way.

The response to the question is as follows:

The National Plan to End Violence against Women and Children 2022-2032 (National Plan) is committed to ending gender-based violence including by addressing the ways technologies are used as a tool to enact family, domestic and sexual violence. Action 6 of the First Action Plan 2023-2027 focuses on addressing all forms of sexual violence and harassment. Technology facilitated abuse (TFA), which includes image-based abuse, is recognised as a form of gender-based violence in the National Plan.

The Australian Government funds online safety initiatives that focus on preventing gender-based violence in all its forms including through raising awareness and understanding, as well as encouraging the use of technology as a positive, protective factor. Initiatives include:

- $3 million over 4 years (2021-22 to 2024-25) for the eSafety Commissioner (Commissioner) to provide targeted support for children experiencing TFA. This includes resources to help adults, such as frontline workers and educators, work with children to identify early warning signs of technology-facilitated abuse, and develop and implement strategies to manage the effects of abuse and assist them to seek support.

- The Preventing Tech-based Abuse of Women Grants Program is providing $10 million through at least three grant rounds to support projects that aim to address or prevent tech-based abuse against women and their children. Applications for Round 1 of the Preventing Tech-based Abuse of Women Grants Program opened on 18 April 2023 and closed on 29 May 2023. A total of $3 million was awarded to successful organisations. Further details of round one grants projects can be found here: https://www.esafety.gov.au/about-us/what-we-do/our-programs/esafety-grants/preventing-tech-based-abuse-grant-program-round-1-recipients.

- Noting the intersections between prevention with intervention and response, eSafety has received $16.6 million over four years (2022-23 to 2025-26) to develop a support service for technology-facilitated family, domestic and sexual violence (TFA-FDSV). The service design and research phase of this project has included user-centred research and service design, extensive consultation with key stakeholders including convening an Expert Advisory Panel, publishing a literature scan and new and updated website guidance on TFA-FDSV. eSafety is now preparing to launch a pilot of the service based on the outputs of the research and service design phase.

The Australian Government also funds a number of sexual violence and online safety initiatives as part of its $3.4 billion commitment to implementing the National Plan. It provides funding to prevention and response to sexual violence through a number of programs and initiatives including Teach Us Consent (Promoting Consent Initiative), *Consent Can't Wait* campaign, *The Line*, *Stop it at the Start* campaign, Community-led Sexual Violence Prevention Pilots, Healthy Masculinities Trial and Evaluation (Healthy MaTE), LGBTIQA+ Sexual Violence Response Pilots, Respect & Equality Initiative (Our Watch), Respect@Work Review (Recommendations 4,5,7,8,13, and 54), Forced Marriage Specialist Support Program, Speak Now, Monash University accredited training for medical and non-medical frontline workers, and 1800RESPECT. In addition, some programs provide support across all aspects of family, domestic and sexual violence such as the Escaping Violence Payment trial, which will become the Leaving Violence Program as announced in the 2024-25 budget.

States and territories have primary responsibility for frontline service delivery. The Australian Government is investing $159.0 million over two years from 2023-24 for the National Partnership on Family, Domestic and Sexual Violence Responses (FDSV National Partnership), with state and territory governments to support frontline family, domestic and sexual violence services. This investment builds on the $270.7 million provided over two years from 2021-22 under the FDSV National Partnership. States and territories are responsible for distributing the funding under the FDSV National Partnership to services based on needs in their jurisdictions, including sexual violence services.

Senate Legal and Constitutional Affairs Legislation Committee

Attorney-General's Department

Hearing date: 23 July 2024

Hansard page: 49-50

Larissa Waters asked the following question:

Senator WATERS:...The last question is: who has the power, if anyone—and it doesn't exist at the moment—to simply deplatform particular apps that can only have a nefarious purpose, like the Nudify apps that have come up quite a bit in discussion today? The eSafety Commissioner took that on notice but I think said, in essence, that she doesn't have that power already but she would welcome it. Does anybody else have that power? And is government considering giving anybody that power? What work has been done in that regard?

The response to the question is as follows:

The Online Content Scheme, established by the *Online Safety Act 2021* (Online Safety Act), empowers the eSafety Commissioner to issue an app removal notice in specific circumstances. This power is targeted at restricting access to Class 1 material[1] (rather than at deepfakes specifically or at apps used to generate deepfakes).

Under Section 128 of the Online Safety Act, if:

- a person provides an app distribution service (eg. an app store); and
- the service enables Australian end-users to download an app that facilitates sharing of Class 1 material

the eSafety Commissioner may issue a written notice to the app distribution service requiring them to make the app unavailable to Australian users within 24 hours. Failure to comply may result in a civil penalty of up to 500 penalty units.

In order to issue this notice, the eSafety Commissioner must:

- be satisfied that there were two or more times during the previous 12 months when Australian end-users could use the service to download an app that facilitiates sharing of Class 1 material; and

[1] Class 1 material is material that is or would likely be refused classification under the National Classification Scheme. It includes material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not), or
- promotes, incites or instructs in matters of crime or violence.

- have given one or more notices under section 109 or 110 of the Online Safety Act in relation to class 1 material, which were not complied with.

Online Safety Act Review

On 22 November 2023, the Minister for Communications, the Hon Michelle Rowland MP, announced the commencement of a statutory review into the operation of the Online Safety Act 2021 (the Act). Ms Delia Rickard PSM was appointed to conduct the review and provide a report to the Minister by 31 October 2024.

The Review is a broad-ranging examination of the effectiveness of the Act, and will consider whether additional protections are needed for harmful online material such as online hate and image-based abuse.

It will consider the need for further protections to address online harms stemming from new and emerging technologies like generative artificial intelligence (including deepfakes) and algorithms, and whether the existing penalty regime works as an effective deterrent to industry non-compliance.

This response has been prepared in consultation with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Senate Legal and Constitutional Affairs Legislation Committee

Attorney-General's Department

Hearing date: 23 July 2024

Hansard page: 50

Larissa Waters asked the following question:

Senator WATERS: Lastly, who does the ratings on the age appropriateness of the apps that people can download? We heard one of the witnesses say that a particular app that had been used for image-based abuse had been initially classified as appropriate for four years plus. That's clearly not right. I hope the answer isn't that the app creators themselves classify themselves, because that's clearly not working. Who does that classification and what input can the federal government have to make sure that those ratings are more appropriate and promote online safety?

The response to the question is as follows:

Under the National Classification Scheme (the Scheme), applications are able to be classified by third parties through the use of ministerially approved classification tools.

Successive reviews have found that the Scheme has not kept pace with the way Australians access media content, particularly the rapid growth in digital and online content and the emergence of new content sharing platforms and interactive features, or with evolving community standards.

In March 2023, the Australian Government announced a two-stage reform process to the Scheme. The first stage of reforms commenced on 14 March 2024, and includes expanding options for industry to self classify content, supported by oversight from the Classification Board, and removing the need to re-classify content already classified for broadcast television.

The next stage will consider comprehensive reform to the Scheme, including potential changes to clarify its purpose and scope, and establish fit-for-purpose regulatory and governance arrangements. Consideration will also be given to classification criteria and responsiveness of the Scheme to evolving community standards, expectations and evidence. This stage of reform will also consider the outcomes of the *Online Safety Act 2021* Review.

This response has been prepared in consultation with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.