Australian Government
Attorney-General's Department

June 2024

Parliamentary Joint Select Committee on Social Media and Australian Society

The influence and impacts of social media on Australian society

Introduction

The Attorney-General's Department (the department) welcomes the opportunity to make a submission to the current inquiry by the Parliamentary Joint Select Committee on Social Media and Australian Society.

The Committee's terms of reference raise issues relevant to a range of the department's legislative, policy, and operational responsibilities and ongoing work to address challenges faced by the Australian community online. While the widespread adoption of social media creates opportunities for connection and engagement within Australian society, it also poses substantial and novel risks, including risks to child safety, privacy, law enforcement and security. Work conducted by the department and its portfolio agencies is critical to combatting and mitigating these risks.

The National Office of Child Safety (NOCS) within the department is leading broader efforts to counter online child exploitation and abuse throughout the community. The department is also leading work to implement the Government's Response to the Privacy Act Review, which includes proposals to strengthen privacy protections for children and introduce a Children's Online Privacy Code. The Government has agreed in-principle to consider reforms to the Privacy Act to regulate how personal information is used for the purposes of digital platforms and other entities recommending content and serving targeted advertising to individuals, including by prohibiting or restricting harmful practices and by requiring greater transparency about the use of these practices.

The department is also working with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts which is leading work to explore the use and implementation of age assurance services for social media. 'Age assurance' is an umbrella term which includes both age verification and age estimation solutions. Age verification measures determine a person's age to a high level of certainty, whereas age estimation technologies provide an approximate age or age range. Age assurance services would seek to protect children from being exposed to harmful or inappropriate material online. Age assurance should be undertaken in a way that does not incentivise entities to collect and retain more personal information than is necessary to verify or estimate their age.

The Government has also introduced new criminal offences to target the creation and distribution of non-consensual 'deepfake' sexually explicit material to counter online hate and extremist material spread across social media platforms. The department is also working with stakeholders including portfolio agencies, international partners and industry, to meet the challenges posed by end-to-end encryption (E2EE) and other anonymising technologies.

Combatting harmful online behaviours

Online child sexual exploitation and abuse

Online child sexual exploitation and abuse has become more prevalent, commodified, organised and extreme, with the Australian Centre to Counter Child Exploitation reporting a 185 per cent increase in the number of suspected child sexual abuse reports since its inception in 2018. The National Centre for Missing Exploited Children, a United States-based global information clearinghouse that receives reports of suspected child sexual exploitation including from Australia, reported the number of reports it analysed grew from 16.9 million in 2019 to over 36 million

reports in 2023. On average, 250 child victims of sexual extortion report their abuse to the Australian Centre to Counter Child Exploitation each month.

With 96 percent of Australians connected to the internet, the high internet penetration rate and significant uptake and popularity of social media and internet applications amongst children has afforded offenders a direct line to groom, coerce and exploit victims at scale.

Australia has a comprehensive framework of offences relating to online child sexual exploitation and abuse. The department works closely with other Commonwealth agencies, including the AFP, to monitor the legislative framework to ensure it is comprehensive, reflects the needs of police and prosecutors, keeps pace with emerging trends and technology, and supports victims. This includes progressing measures under the First Commonwealth Action Plan of the *National Strategy to Prevent and Respond to Child Sexual Abuse 2021-2030* to review Commonwealth child abuse offences to ensure they remain current and reflect emerging trends (Measure 13).

Noting offenders can manipulate and coerce a child into performing a sexual act within ten minutes of contact, safeguards must be adopted by online service providers to reduce the risk of child sexual exploitation. Age-gates are largely insufficient to prevent children from accessing social media, or online content that is not age appropriate (including pornography), as users can easily bypass this measure by claiming they are a different age without any assurance checks. Despite social media platforms stipulating in their terms of use that users must be over the age of 13 to use their platforms, many children under the age of 13 have unfettered access to all content and features on these applications due to poor age assurance standards.

Age assurance should be considered to protect children from being exposed to inappropriate content, including harmful behaviours in pornography that can lead to the de-sensitisation and normalisation of sexual violence, and harmful sexual dynamics. Age assurance should also be applied to identify users who are children, and safeguard them from being contacted from unknown adult users on the same online platform/application. Age assurance can further be utilised to support online service providers to identify users under the age of 18, and tailor privacy protections, location tracking, user findability, and recommender systems to these users to better protect them from adult offenders and other malicious actors.

Noting major online service providers and social media platforms are signatories to global online safety efforts such as the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, governments and law enforcement agencies continue to see the rollout of new features and technologies that undermine the safety of children. Options to encourage mandatory uplift of online safety standards, including age assurance, to ensure the best interests of the child are prioritised in the design of platforms and services would strengthen protections.

Malicious sharing of personal information online (doxxing)

The rapid advancement of technology and the prevalence of social media have contributed to increases in harmful behaviours like doxxing: the malicious publication of an individual's private information online Doxxing can leave targets vulnerable to, and fearful of, public embarrassment, humiliation or shaming; discrimination; stalking; identity theft and financial fraud; and damage to their personal and professional reputation. The Government has announced that it will bring forward new offences in August 2024 to address doxxing, along with a new statutory tort for serious invasions of privacy, and reforms to the Privacy Act to ensure Australians have greater control and transparency over their personal information.

Non-consensual sharing of sexually explicit material online

In recent years, emerging technologies such as artificial intelligence (AI), are being used to produce deepfakes, which are extremely realistic, but false, depictions of real people. This can include deepfakes of real people in sexual contexts, which can be used to harass, intimate, blackmail, coerce and humiliate victims.

The non-consensual sharing of both real and artificially generated sexual material online is becoming increasingly harmful as technologies, such as AI, become more accessible, user friendly and ubiquitous. The creation of fake sexual material poses significant risks to the Australian community, and the non-consensual sharing of this material can have long-lasting harmful impacts on victims. Such conduct is often targeted at women and girls and used to perpetrate gender-based violence online.

On 5 June 2024, the Attorney-General, the Hon Mark Dreyfus KC MP, introduced the Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 to modernise and strengthen offences for the non-consensual sharing of simulated and real sexual material online. The reforms ensure that the online sharing of sexually explicit material without consent, including material generated or altered using technology (like AI-generated deepfakes), is subject to appropriate criminal penalties. Aggravated penalties will apply where the person was also responsible for the creation or alteration of the sexual material transmitted.

Sharing of abhorrent violent material

Subdivision H of Part 10.6 of the *Criminal Code Act 1995* makes it an offence for internet service providers and hosting and content providers to fail to remove access to abhorrent violent material expeditiously where the material is reasonably capable of being accessed within Australia. It is also an offence for content service and hosting services to fail to notify the Australian Federal Police within a reasonable time about material relating to abhorrent violent conduct occurring in Australia. Abhorrent violent material is limited to very specific categories of the most egregious, violent audio, visual or audio-visual material produced by a perpetrator or their accomplice. It must stream or record actual acts of murder, rape, torture, terrorism involving physical harm and/or violent kidnaping. It also must be material that reasonable persons would regard as being, in all the circumstances, offensive.

These offences target social media providers who are aware of abhorrent violent material that can be accessed through their service and fail to act. Failure to notify attracts civil penalties, and failure to remove material can attract both civil penalties and up to 3 years' imprisonment for individuals.

These offences complement the eSafety Commissioner's powers to issue a removal notice to any website publishing abhorrent material and/or the service that hosts the website. The department notes the review of the *Online Safety Act 2021* is currently underway and is considering the effectiveness of the Act and whether additional protections are needed for harmful online material such as online hate and image-based abuse.

Online hate

In January 2024, new offences in the Criminal Code enacted through the *Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Act 2023* (Prohibited Hate Symbols Act) came into force. These offences are for the public display of prohibited Nazi and terrorist organisation symbols, the making of a gesture that is the Nazi salute, using a carriage service for violent extremist material, and possessing or controlling violent extremist material obtained or accessed using a carriage service.

The offences may capture conduct in relation to content disseminated over social media. The prohibited symbols and salute offences apply to conduct in a 'public place', which is defined in the Criminal Code Dictionary. The explanatory memorandum to the Prohibited Hate Symbols Act specifies that the definition of 'public place' is intended to capture both physical and online places.[1] The violent extremist material offences apply where a carriage service is used in relation to the violent extremist material, including to access or distribute the material. The explanatory memorandum outlines that use of a carriage service includes use of the internet and social media applications.[2]

The offences were enacted to facilitate law enforcement intervention at an earlier stage in individuals' progress to violent radicalisation, and provide greater opportunities for rehabilitation and disruption of violent extremist networks. The offences are also intended to complement the existing framework for regulating online service providers, including offences for hosting abhorrent violent material.

Earlier this year, the Attorney-General announced that the Government would bring forward legislation to strengthen current laws that deal with hate speech. The Government is committed to pursuing legislative amendments to create new criminal offences and strengthen existing laws relating to hate speech. The laws would protect the community from those who promote extremism, hatred or seek to incite violence.

Protecting Australians online

Privacy Act reforms

The *Privacy Act 1988* protects individuals' personal information and regulates how Commonwealth agencies, organisations with a turnover of over $3 million per year, and some smaller entities, can collect, use, disclose and handle personal information. On 28 September 2023, the Government released its Response to the Privacy Act Review[3] outlining its views on a broad range of proposals to ensure Australia's privacy framework is fit for purpose in the digital age, aligns with global standards of personal information protection and appropriately addresses current and emerging privacy risks. Of particular relevance to the current Inquiry are the following proposals:

- Updating and clarifying the definition of 'personal information' to ensure that it includes technical and inferred information (such as IP addresses and device identifiers) where this information can be used to identify individuals[4]
- requiring that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.[5] Entities should also be required to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances,[6] amongst other considerations

[1] See paragraph 266 of the revised explanatory memorandum to the Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Bill 2023.
[2] See paragraph 308 of the revised explanatory memorandum to the Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Bill 2023.
[3] Government Response to the Privacy Act Review Report, 28 September 2023 < https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>
[4] Proposals 4.1–4.5, 4.9, Government Response to the Privacy Act Review Report.
[5] Proposals 12.1–12.3, Government Response to the Privacy Act Review Report.
[6] Proposal 16.4, Government Response to the Privacy Act Review Report.

- introducing a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'[7]
- codifying the principle that valid consent must be given with capacity[8]
- requiring entities to obtain consent to collect geolocation tracking data[9]
- increasing transparency and integrity of decisions made using personal information in automated decision-making systems, and giving individuals a right to request meaningful information about how automated decisions with legal or similarly significant effect are made[10]
- targeting individuals should be fair and reasonable in the circumstances, and targeting individuals based on sensitive information should be prohibited, with appropriate exceptions[11]
- prohibiting entities from[12]:
    - targeting to a child, with an exception for targeting that is in the child's best interests,
    - trading in the personal information of children, and
    - direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests, and
- requiring entities to provide information to online users about the use of targeting systems, including clear information about the use of algorithms and profiling to recommend content to individuals[13].

The Privacy Act does not currently contain specific protections for children. Children are particularly vulnerable to privacy harms online, and digital platforms (and others) can handle children's personal information in invasive and harmful ways. To address these issues, the Government has agreed or agreed in-principle to consider specific privacy protections for children, including providing for development of a Children's Online Privacy Code.

To meet new privacy requirements in relation to children, it is expected that entities will need to take a risk-based approach to establishing an individual's age with a level of certainty that is appropriate to the privacy risks, for example by implementing age assurance. The Office of the Australian Information Commissioner (OAIC) has issued guidance to help entities to decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, as a general rule, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

The Government Response to the Privacy Act Review acknowledged the importance of individuals having more choice and control in relation to their own information, and noted that the proposal to provide individuals with an unqualified right to opt-out of receiving targeted advertising (proposal 20.3) is directed to achieving this objective. Further consideration is being given to how to give individuals more choice and control in relation to the use of their information for targeted advertising.

[7] Proposal 16.5, Government Response to the Privacy Act Review Report.
[8] Proposal 16.2, Government Response to the Privacy Act Review Report.
[9] Proposal 4.10, Government Response to the Privacy Act Review Report.
[10] Proposals 19.1–19.3, Government Response to the Privacy Act Review Report.
[11] Proposal 20.8, Government Response to the Privacy Act Review Report.
[12] Proposals 20.5–20.7, Government Response to the Privacy Act Review Report.
[13] Proposal 20.9, Government Response to the Privacy Act Review Report.

The Privacy Act Review had noted that targeting can lead to consumer harms through:

- the delivery of highly personalised and targeted advertisements to vulnerable consumers, including children, for alcohol, gambling, or unhealthy food and beverages
- impacting an individual's autonomy by reinforcing existing preferences and shaping new ones
- contributing to disinformation campaigns or discriminating against certain groups or individuals, and
- serving increasingly extreme content because a person has viewed similar material, or prioritising controversial, shocking or extreme content that produces emotional responses.

The Government has also agreed in-principle to address harmful targeting practices by giving individuals greater choice and control, prohibiting certain practices, and increasing awareness and understanding about how targeting systems work so individuals can understand why they are being targeted with certain advertising and content. These issues will be considered further as part of the Government's consideration of reforms to the Privacy Act.

End-to-end encryption and lawful access to data

The department also notes there has been a significant increase in the uptake of E2EE by social media companies in recent years in response to the growth of cybercrime and increased threat of malicious actors. Examples of services that have adopted E2EE include iMessage, WhatsApp, Signal, and parts of Skype and Telegram, and Meta is in the process of implementing it across its Facebook and Instagram messaging services.

In early 2024, the AFP reported 96.1 per cent of lawfully intercepted communications content was unintelligible due to E2EE, and ASIO stated that E2EE damages intelligence coverage in virtually 100% of its priority counter-terrorism and counter-espionage cases. In April 2024, the Director-General of the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) Commissioner emphasised the impact of encryption on their investigations and likened it to creating a 'safe room for terrorists and spies'. In his speech, the Director-General made it very clear that agencies are not asking for new powers or more resources but for technology companies to do more to give effect to existing powers and to uphold existing laws.

More needs to be done by social media companies to ensure that they are able to protect users and assist law enforcement to investigate serious offences, such as child sexual abuse. The department is working collaboratively with Five Eyes partners and industry to find a solution that preserves social media companies' ability to innovate, while still maintain tightly controlled lawful access.

Copyright, artificial intelligence, and social media

As a related matter that may be of interest to the Committee, the department is currently engaging with diverse stakeholders – including from across the creative, media and technology sectors – to review the intersection between copyright law and artificial intelligence (AI) and develop evidence-based policy options for consideration by government. This is occurring primarily through consultation with the Copyright and AI Reference Group announced by the Attorney General in December 2023. Participants in the Reference Group

include representatives of companies that operate social media platforms and Australian journalism, news and media organisations.

An initial focus of the department's consultation with the Reference Group is the use of copyright material as inputs for AI systems. This is a complex and sensitive issue in Australia and internationally, which requires consideration in a careful and consultative manner. Other topics intended to be explored in consultation with the Reference Group in 2024 include issues regarding potential copyright infringement in the outputs of generative AI systems and the copyright status of AI outputs.

Points of potential intersection with matters being considered by the Committee may include:

- *The use for AI training of copyright-protected content posted to social media platforms by users*. Social media platform terms of service often require users to grant the providers non-exclusive, royalty-free licences to the provider to use any content they upload for the purposes of providing and improving its products and services. There has been recent media attention on amendments to some providers' terms of service relating to the use of user-uploaded content to improve AI systems.
- *Transparency around the use of copyright material as AI inputs*. Numerous creative industries and other copyright owner stakeholders, including in the journalism, news and media sectors, have called for greater transparency around when their material is used as inputs in the training and operation of AI systems.