

Communications Law Bulletin

Contents

- 3 An Update on Australia's Privacy Reforms
- 5 A Spotlight on Australian Privacy Reform: A Long Awaited First Step – First Tranche Privacy Reforms Introduced to Parliament
- 9 Data Breaches Up, So Protecting Yourself is Crucial, Says New OAIC Report
- 10 Book Review - *Rolph on Defamation 2nd Edition* by Professor D Rolph
- 11 Interview with Jason Qian
- 12 Event Report: CAMLA Cup
- 13 Game Over, or a Glitch? The Potential Copyright Concerns with Integrating AI-Generated Assets in Video Games
- 16 Birkenstock Shows That it is Possible to Secure Trade Mark Protection Over the Shape of Popular Product Designs
- 19 Legislation Introduced to Combat Mis- and Dis-information on Online Platforms
- 21 Australian "Social Media" Age Restrictions May Be on the Way with South Australia Championing Reform
- 23 "Consent or Pay" Models Under Scrutiny in UK and EU
- 25 Top of the Menu: ACMA Puts Free-to-air in the Spotlight with New TV Prominence Framework
- 28 Event Report: CAMLA Young Lawyers Committee - Media, Law & The Games Seminar
- 29 Responsible Use of AI: New Australian Guardrails Released
- 31 The Proposed Scams Framework: A Whole of Ecosystem Approach to Protecting Australians from Scams
- 34 Important Cyber Security Reforms Tabled in Parliament and Referred to Committee

Editors

Ashleigh Fehrenbach
and Eli Fisher

Editorial Assistants

Jeren Gul and
Daniella Lambert

Editors' Note

Dear Readers,

We are excited to present a collection of articles, interviews and even a book review, that explore the latest issues and developments in privacy, data protection, digital platforms, trade marks and copyright and AI.

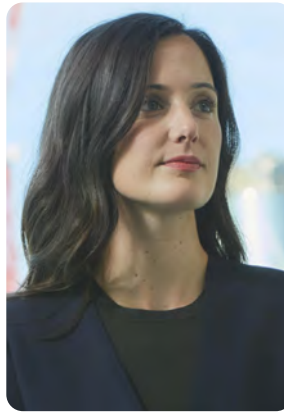
First up, we'll hear from Australian Privacy Commissioner, **Carly Kind**, on the Federal Government's first tranche of reforms to the *Privacy Act 1988*, and why these changes are so needed. The team at **Bird and Bird** (**Julie Cheeseman**, **James Hoy**, **Emma Croft**, **Jonathan Tay**, **Evelyn Park** and **Ruby Simpson**) carefully step us through what the three key categories of reform mean for our national privacy laws and we can expect in on the next tranche.

Clayton Utz's Brenton Steenkamp, **Utsab Banskota** and **Deepa Thakkar** examine the OAIC's recent and latest Notifiable Data Breach guidance and what actionable considerations organisations should be taken to guard against Australia's increasing data breach count. On a related note, scam activity is also on the rise, with Australians losing \$2.74 billion to scammers in 2023. **Antonia Garling**, **Silvana Good** and **Jeremy Jose (G+T)** brief us on Australia's proposed new scams prevention framework aimed at protecting Australians from escalating scam threats.

Further on the regulatory front, the OAIC has notably closed its investigation into 7-Eleven Stores following a 2021 privacy breach incident. **JWS' Sophie Dawson**, **John Keeves** and **Bianca Collazos** report on the OAIC's decision as well as the recent Cyber Security Legislative package tabled to Parliament, and what it means if the legislation is passed. Meanwhile the team at **Clayton Utz** (**Timothy Webb**, **Joel Parsons** and **Chelsea Manansala**) take a look into ACMA's public consultation regarding the television framework, offering insights into the regulatory environment for broadcasting in Australia.

Taking stock on AI developments, **MinterEllison's Sonja Read**, **Shane Evans**, **Chelsea Gordon** and **Sam Burrett** provide us with a breakdown on the two new Government publications which seek to guide the development and deployment of AI in Australia. We also have **Sol Bedi** from **Cam Rogers Legal** posing the question, "Game Over, or a Glitch?" and exploring the potential copyright concerns associated with the integration of AI-generated assets in video games. This timely examination is particularly relevant as the gaming industry continues to develop alongside rapid tech advancements.

On digital platforms, we have **Addisons' Justine Munsie** and **Brodie Campbell** unpacking the objectives of Australia's proposed *Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2024 (Cth)*. Many are asking if the Bill has struck the right balance when it comes to free speech – a question that folks are also asking with respect to South Australia's potential age restrictions on social media. The **JWS** team, (**Sophie Dawson** and **Hamish Lennon**) take us through the Honourable Robert French AC's 'Report of the Independent Legal Examination into Banning Children's Access to Social Media' and the South Australian consultation exposure draft of the Children (Social Media Safety) Bill. **Gaden's Jeren Gul** takes hold of the mic to



Ashleigh Fehrenbach



Eli Fisher

interview **Tik Tok Legal Counsel, Jason Qian** on his career to date. To round out developments on social media, **RPC's Oliver Bray** and **Ashleigh Fehrenbach** provide us with an analysis of the proposed "consent or pay" models under scrutiny in the UK and EU.

For developments in trade marks we have **Clayton Utz's Connie Beswick** and **James Neil** discussing the recent Birkenstock case, highlighting the significance of securing trade mark protection for product design shapes. Spoiler: Fear not, your favourite Birks, whether they be the "Arizona", the "Madrid" or the uber chic "Boston", are safe and sound.

We are also very pleased to include a review of **Professor David Rolph's** insightful book, '*Rolph on Defamation, Second Edition*'. The review, written by Her Honour Justice Gleeson, reflects on Professor Rolph's valuable examination of the fundamentals of defamation law.

When it comes to seminars and events, it should come as no surprise that CAMLA has been busy. On 30 October, Ashurst hosted CAMLA's Part 3 on 'The Future of Australian Content'. In the following pages, you'll hear all about CAMLA Young Lawyers' incredibly successful '**Media Law and the Games**' seminar (with **Tara Hayes** reporting) and the gem of CAMLA's social calendar, **CAMLA Cup**, reported on by **Alana Callus**. Thank you to all those who attended these events and seminars! A huge thank you in particular to the following organisations, who kindly donated our CAMLA Cup prizes: ABC, Addisons, Allens, Ashurst, Baker McKenzie, Banki Haddock Fiora, Bird & Bird, Creative Lawyers, Clayton Utz, Dentons, Foxtel, Free TV, Gadens, Gilbert + Tobin, Herbert Smith Freehills, HWL Ebsworth, Johnson Winter Slattery, Level 22 Chambers, Marque, MinterEllison, Netflix, Seven, Thomson Geer, TikTok, Optus and Webb Henderson.

We still have a stacked calendar as we run into the final months of the year. CAMLA Young Lawyers are organising an upcoming **Fashion 101 panel**, keep an eye out for the details. 14 November marks the date of our **Annual Oration** and this year, **His Honor Justice Lee** will be presenting the keynote speech on "Contemporary Challenges with Open Justice" – there's still time to register your spot! Finally, on 5 December, we hope you'll join us for CAMLA's celebratory **End of Year Drinks** hosted by G+T.

Happy reading!

Eli and Ash

An Update on Australia's Privacy Reforms

Author: Australian Privacy Commissioner, **Carly Kind**

The first tranche of privacy reforms announced by the Federal Government to the Privacy Act 1988 are very welcome and an important first step, but it is clear that more will need to be done if we want a privacy framework that can deal with the privacy challenges of tomorrow.

The Bill, that is now before Parliament, will:

- strengthen the OAIC's enforcement toolkit, which will include a new mid-tier civil penalty for interferences with privacy and a low-level civil penalty provision for specific administrative breaches of the Act with attached infringement notice powers;
- require the OAIC to develop a new Children's Online Privacy Code to enhance privacy protections for children in the online environment, particularly when using digital platforms;
- Require entities to include information in privacy policies about automated decisions that significantly affect the rights or interests of an individual; and
- introduce a statutory tort for serious invasions of privacy, which would be an important addition to the suite of regulatory measures needed to address gaps in the existing privacy protection framework and address current and emerging privacy risks and harms (such as doxxing).

For a modern regulator, it's essential to have enforcement measures available that can maximise our flexibility, so that we can apply a risk-based approach to enforcement that is proportionate and also supportive of a growing digital economy.

The statutory tort will also fill a gap in our privacy landscape by providing people with the ability to seek redress through the courts for serious invasions of privacy without being limited to the scope of the Act.

Children's Online Privacy Code

It is a fact that the Privacy Act itself has not kept pace with the adoption of digital technologies and the privacy risks and harms faced by Australians, particularly children and young people, in the online environment.

Children frequently spend time online to connect with friends, learn and be entertained. It is unrealistic to keep kids off the internet in the 21st century. However, online services designed to appeal to young people may not always be safe, appropriate and protect their privacy. We know Australian parents are concerned about this; a survey we conducted last year found 85% of parents believe children must be empowered to use the internet and online services, but their data privacy must be protected.

A key initiative in the Bill is a mandate for the OAIC to develop a Children's Online Privacy Code, which would centre children in the debate around privacy in Australia and help to harmonise protections which those children already benefit from in other countries such as the UK.



As code developer, our ultimate objective is not to prevent children from engaging in the digital world, but rather to protect them within it through strengthened privacy protections for the handling of their personal information.

The code will apply to social media and a wide range of other internet services likely to be accessed by children, including apps, websites and messaging platforms. It will specify how these services must comply with the Australian Privacy Principles, which are the cornerstone of the privacy protection framework in the Privacy Act 1988. The code may impose additional requirements provided they are not inconsistent with the existing principles.

For example, under the Australian Privacy Principles, organisations have obligations to have a privacy policy and to provide collection notices. The code might set out how organisations should tailor privacy policies and collection notices for a child so that they are clear and easy to understand, for example, by using graphics, video and audio content, rather than relying solely on words.

Ultimately, the content of the code will be determined through the code development process. The OAIC intends to adopt a transparent and collaborative approach. We will consult widely with children, parents, child development experts, child welfare advocates, civil society, other regulators and across the online industry to ensure different voices are heard and represented throughout the process.

To the extent possible, we will look to align the code with the UK's Age Appropriate Design Code, while recognising there are differences in the underlying legal frameworks, and leverage the learnings of our international counterparts.

We are also mindful of broader government initiatives, including the proposed introduction of a minimum age for access to social media and other relevant digital platforms, the age assurance trial, the review of the Online Safety Act 2021 and the eSafety Commissioner's ongoing work with industry codes and standards. We will continue working with stakeholders across government, industry and the community to ensure a consistent and complementary approach to addressing online harms for all Australians.

Next steps

Meanwhile, we are eagerly awaiting the second tranche of privacy reforms, dealing with much needed reforms including a new positive obligation that personal information handling is fair and reasonable,

The coverage of Australia's privacy legislation lags behind the advancing skills of malicious cyber actors. Further reform of the Privacy Act is urgent, to ensure all Australian organisations build the highest levels of security into their operations and the community's personal information is protected to the maximum extent possible.

CAMLA ESSAY COMPETITION 2024

Did you write a great media and
communications law essay this year?
Enter it in the 2024 CAMLA essay
competition!

1st Place:

\$1000 + CAMLA Membership + Mentoring Session

2nd Place:

\$600 + CAMLA Membership

3rd Place:

\$400 + CAMLA Membership

ENTRIES DUE: SUNDAY 3 NOVEMBER 2024

For full entry details visit www.camla.org.au

Or email contact@camla.org.au

A Spotlight on an Australian Privacy Reform: A Long Awaited First Step – First Tranche Privacy Reforms Introduced to Parliament

Authors: Julie Cheeseman (Partner), **James Hoy** (Special Counsel), **Emma Croft** (Senior Associate), **Jonathan Tay** (Senior Associate), **Evelyn Park** (Associate) and **Ruby Simpson** (Lawyer), Bird and Bird

On 12 September 2024, the Australian Government introduced the **Privacy and Other Legislation Amendment Bill 2024 (Bill)** to the House of Representatives containing the first tranche of long-awaited reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**).

Arriving almost one year after the Government published its Response to the Privacy Act Review (**Response**) and indicated that a generational overhaul of Australia's Privacy Act was needed, the reforms contained in the Bill are far more limited in scope. The Bill focuses on three categories of amendments to Australia's privacy, regulatory and criminal laws:

1. measures to enhance the privacy of individuals, including by strengthening the Office of the Australian Information Commissioner's (**OAIC**) enforcement toolkit, introducing new tiers of civil penalties, requiring the development and registration of a Children's Online Privacy Code, and increased transparency requirements for automated decision making;
2. the introduction of a new statutory cause of action for serious invasions of privacy; and
3. the introduction of new offences to specifically criminalise 'doxxing'.

Notably, the Bill does not include the most ambitious reforms which the Government had previously 'agreed' or 'agreed in principle' in its Response, such as the removal of the small business exemption, amendment of the definition of 'personal information' (**PI**), the introduction of the controller/processor distinction, the proposed requirement that the collection, use and disclosure of PI be fair and reasonable and new definitions for direct marketing, targeting and trading. Given that the Government plans to further consult regarding the next (and more ambitious) tranche of reforms, we are unlikely to see any further reforms arrive in Parliament until after the 2025 federal election.

If the Bill is passed, it will nevertheless be a significant first step towards Australia's privacy laws being made fit for purpose in the digital age. Our more detailed comments on these three categories of reforms are below.

Category 1 - Measures To Enhance the Privacy of Individuals

The most significant category 1 amendments are new civil penalties and a stronger enforcement toolkit for the OAIC, a new Children's Online Privacy Code, and increased transparency requirements for automated decision making.

Civil penalties and enforcement powers: Schedule 1 of the Bill amends Australia's privacy laws to strengthen the enforcement powers of the OAIC and the Courts by providing the Commissioner and the judiciary with a broader range of enforcement options and new functions and capabilities to address actual or suspected privacy interferences (see Parts 8 - 11 and 13 - 14 of Schedule 1 of the Bill).

If implemented as drafted, these amendments apply to acts done or practices engaged in after commencement. In particular, the Bill proposes to:

- provide guidance on factors which may be taken into account to determine whether an interference with privacy is 'serious', for the purposes of availing the Commissioner of the civil penalty provision for serious interferences of privacy;
- remove the previous civil penalty provision for repeated interferences with privacy (as civil penalties for individual interferences of privacy are proposed to be introduced);
- introduce a new civil penalty for interference with the privacy of an individual, notwithstanding the seriousness of that interference (capped at 2,000 penalty units);
- introduce new civil penalties and the power for the Commissioner to issue infringement notices for breaches of some of the APPs and the preparation of non-compliant eligible data breach statements (capped at 200 penalty units);
- provide a legislative means by which, in court proceedings for serious interferences of privacy, the Court may order an entity pay civil penalties in circumstances where it is satisfied that entity interfered with the privacy of an individual but is not satisfied that the interference with privacy is serious;
- empower the Court, when it has or will determine that an entity has contravened a civil penalty provision under the Act, to make an order to direct the entity to redress or pay compensatory damages for the loss or damage suffered or likely to be suffered by any individual. Individuals have a limitation period of 6 years to apply to the Court for an order of this kind and any amount payable to the individual may be recoverable as a debt;
- empower the Commissioner to conduct a public inquiry into matters relating to privacy, at the direction of the Minister;

- empower the Commissioner to make determinations following an investigation declaring that entities perform any reasonable act or course of conduct to redress forward looking, reasonably foreseeable loss or damage likely to be suffered;
- amend the definition of ‘privacy matters’ which must be included in the Commissioner’s annual report to:
 - limit the statement of the performance of the privacy functions relating to the year referable to the annual report;
 - include details of the number of complaints made to the Commissioner over the year referable to the annual report; and
 - include details of the grounds for the Commissioner’s decision not to investigate complaints over the year referable to the annual report (see Part 12, Schedule 1 of the Bill);
- enable the Commissioner to decide not to investigate a complaint in circumstances where the complaint has already been dealt with by a recognised external dispute resolution scheme (see Part 13, Schedule 1 of the Bill); and
- introduce new monitoring and investigative powers which enable the Commissioner (or its staff) to:
 - monitor certain information and matters, including exercise of entry and inspection powers with either consent or judicial authorisation in the form of a warrant; and
 - investigate things with respect to which a civil penalty provision under the Act has been contravened or is suspected, on reasonable grounds, to have been contravened, including by exercise of entry, search and seizure powers with either consent or judicial authorisation in the form of a warrant.

Increased transparency regarding automated decision making: Part 15, Schedule 1 of the Bill contains amendments introducing requirements for entities to include information in privacy policies about the kinds of PI used in, and kinds of decisions made by, automated decision making systems, where such decisions could reasonably be expected to significantly affect the rights or interests of an individual.

In particular, if entities arrange for computer programs to use PI about individuals to make (or do a thing that is substantially or directly related to making) decisions which could reasonably be expected to significantly affect the rights or interests of those individuals, their privacy policy must contain:

- the kinds of PI used in the operation of such computer programs;
- the kinds of such decisions made solely by the operation of such computer programs; and
- the kinds of such decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs.

The Bill provides the following examples of the kinds of decisions that may affect the rights or interests of individuals:

- a decision made under a provision of an Act or a legislative instrument to grant, or to refuse to grant, a benefit to them;

- a decision that affects their rights under a contract, agreement or arrangement; and
- a decision that affects their access to a significant service or support.

New Children’s Online Privacy Code: Part 4 of Schedule 1 of the Bill contains amendments to the Privacy Act that will promote the right to privacy for children. As well as introducing a new definition of a “child” (as an individual who has not reached 18 years), the Bill will require the Information Commissioner to develop and register an APP code about online privacy for children (the Children’s Online Privacy Code (**COP Code**)). The Commissioner may consult with persons the Commissioner considers appropriate in developing the COP Code. The COP Code:

- will be an enforceable APP code which sets out how one or more of the APPs are to be applied or complied with in relation to the privacy of children;
- will impose obligations to providers of social media services, relevant electronic services or designated internet services (as defined in the *Online Safety Act 2021* (Cth)), where the service is likely to be accessed by children and the entity is not providing a health service, and to entities or a class of entities who are specified in the COP Code;
- can also specify entities, or a class of entities, who will not be bound by the COP Code;
- the Commissioner may make written guidelines to assist entities to determine if a service is likely to be accessed by children; and
- to the extent possible, will align with similar overseas children’s codes, such as the UK’s *Age Appropriate Design Code*.

If the Bill is passed, the Commissioner will be required to:

- make a draft of the COP Code publicly available and invite the public to make submissions within a specified period (which must run for at least 40 days). Then, the Commissioner must consult with the eSafety Commissioner and the National Children’s Commissioner; and
- develop and register the COP Code within the period of 24 months beginning on the day the amending legislation receives Royal Assent (i.e. we anticipate if the Bill is passed in 2025, the COP Code will be in force by 2027).

The Government has also announced that, if the COP Code amendments are passed, the OAIC will be provided AU\$3 million over 3 years to assist with the development of the COP Code.

Currently, it is unclear whether the remaining recommendations which received in-principle support (such as direct marketing, targeting and trading of the PI of children (see our previous article [here](#))) will be addressed by the draft COP Code, or whether they will be released with next tranche of reforms.

Any exceptions to the COP Code obligations will likely be addressed in the draft COP Code.

Other category 1 amendments

In addition, other category 1 amendments include:

- **Clarification of Privacy Act objects:** Amendments to the objects of the Privacy Act to clarify that they include promoting the protection of individual's PI, and to recognise the public interest in protecting privacy (see Part 1, Schedule 1 of the Bill).
- **Enhanced code making powers:** Amendments which provide greater flexibility and efficiency to the existing APP code-making processes by empowering the Information Commissioner to develop and register codes or temporary codes if directed to do so by the Minister (see Part 2, Schedule 1 of the Bill).
- **Targeted emergency declarations:** Amendments to the Privacy Act's existing emergency/disaster declaration provisions requiring that they specify the kinds of PI that may be handled, the types of entities permitted to collect, use or disclose the information, and the purposes for which that PI may be collected, used or disclosed (see Part 3, Schedule 1 of the Bill).
- **Security, retention and destruction of PI:** Amendments to APP 11 to include a new subclause 11.3 which clarifies that the steps that entities should consider when determining how they should protect PI should include both technical and organisational measures (see Part 5, Schedule 1 of the Bill).
- **Overseas disclosures of PI:** Amendments to introduce a mechanism by which countries and binding schemes that provide substantially similar privacy protections to the APPs can be prescribed (see Part 6, Schedule 1 of the Bill).
- **Eligible data breach declarations:** Amendments to include new provisions in Part IIIC of the Privacy Act to facilitate information sharing where there has been an eligible data breach of an entity in order to prevent or reduce the risk of harm arising from misuse of PI. The amendments would give a new power to the Minister to make a written declaration enabling specified entities to handle PI in a manner that would otherwise not be permitted under privacy and secrecy laws (e.g. by disapplying the protections that would otherwise apply to the collection, use or disclosure of PI) in order to prevent or reduce the risk of harm to individuals in the event of an eligible data breach. Other amendments include a range of safeguards to minimise potential adverse privacy impacts of the new declaratory power (see Part 7, Schedule 1 of the Bill).

2. New Statutory Tort for Serious Invasions of Privacy

The Bill would also introduce a new statutory tort for serious invasions of privacy, as 'Schedule 2' to the Privacy Act. To establish a cause of action under the proposed statutory tort, it is proposed that a plaintiff must prove four essential elements, as follows:

1. the defendant invaded the plaintiff's privacy by doing one or both of the following:
 - intruding upon the plaintiff's seclusion (e.g. by physically intruding into the plaintiff's private space, or by watching, listening to, or recording their private activities or private affairs); or
 - misusing information that relates to the plaintiff (including but not limited to the collection, use or disclosure of information about the plaintiff), whether that information is true or not;
2. a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances;
3. the invasion of privacy was committed intentionally or recklessly; and
4. the invasion of privacy was serious. By way of example, when considering seriousness, a court may take into account:
 - the degree of any offence, distress or harm to dignity that the invasion of privacy would likely cause to a person of ordinary sensibilities in the position of the plaintiff;
 - whether the defendant knew or ought to have known that the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff; and
 - if the invasion of privacy was intentional—whether the defendant was motivated by malice.

Significantly for defendants who might be subject to a claim following the occurrence of a data breach, the invasion of privacy tort is actionable without proof of damage.

Where a defendant adduces evidence that there was a public interest in the invasion of privacy (e.g. on the grounds of freedom of expression, including political communication, freedom of the media, the proper administration of government, open justice, public health and safety, national security, the prevention and detection of crime and fraud), the plaintiff must satisfy the court that that the public interest was outweighed by the public interest in protecting the plaintiff's privacy;

Defences to the plaintiff's claim are proposed to include the following:

- **Authorisation by law:** where the invasion of privacy was required or authorised by or under an Australian law or court/tribunal order;
- **Consent:** the plaintiff (or someone authorised on their behalf) expressly or impliedly consented to the invasion of privacy;
- **Health, life or safety:** the defendant reasonably believed that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person;
- **Defence of person or property:** the invasion of privacy was:
 - incidental to the exercise of a lawful right of defence of persons or property; and
 - proportionate, necessary and reasonable.
- **Defamation overlap:** where the defendant would be able to establish the defence of absolute privilege, publication of public documents, or fair report of proceedings of public concern in relation to information published about the plaintiff if the claim was brought under an Australian law that deals with defamation.;

Exemptions apply in relation to an invasion of privacy:

- by a journalist, the journalist's employer, or certain persons assisting the journalist to the extent the invasion involves the collection, preparation for publication or publication of journalistic material;
- by an enforcement body to the extent that the body reasonably believes that the invasion of privacy is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
- by intelligence agencies, or to the extent the invasion involves the disclosure of information to or by an intelligence agency; and
- by a person who is under 18 years of age.

As for relief, Courts would be entitled to grant injunctions (including interim injunctions), give summary judgment, award damages (including for emotional distress but not aggravated damages), exemplary or punitive damages (in exceptional circumstances), an account of profits, orders requiring an apology from the defendant, correction orders, destruction orders and declarations.

Damages awarded for non-economic loss and exemplary/punitive damages, are proposed to be capped at the amount that is the greater of \$478,550 or the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law.

Other than in particular circumstances, plaintiffs will be required to commence proceedings within 3 years of the invasion of privacy occurring or (for plaintiffs that were 18 or over at the time of publication) within a year of becoming aware of the invasion (whichever is earlier).

Relevantly for international organisations carrying on business in Australia, the extra-territorial provisions are proposed not to apply to the statutory tort.

3. Criminal Offences Targeting 'Doxxing'

The Bill also includes amendments to the *Criminal Code Act 1995* (Cth) to introduce new criminal offences to target 'doxxing', which is a form of abuse that disproportionately affects women. 'Doxxing' refers to the publication or distribution of personal data using a carriage service in a manner that reasonable persons would regard as being menacing or harassing. 'Personal data' in this context refers to information about an individual that enables that individual to be identified, contacted or located, such as their name, photograph, telephone number, email address, online account information, residential or work address, and place of education or worship.

The Bill would introduce an offence carrying 6 years' imprisonment, and a further, more serious offence carrying 7 years' imprisonment if the individual or group of individuals is targeted because of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality, or national or ethnic origin. These penalties are consistent with the penalties introduced in June 2024 for the creation and sharing of sexually explicit material (including deepfakes) without consent.

What's Next

Debate on the Bill has been adjourned (and made an order of the day for the next sitting). However, with only limited sittings remaining in 2024, there is a distinct possibility the Bill will not pass this calendar year.

The next tranche of (more ambitious) reforms will be the subject of further consultation by the Government and is unlikely to reach Parliament before the 2025 federal election.

Notwithstanding the above, some key takeaways for entities already regulated by the Privacy Act are that:

- Privacy enforcement risk remains high in Australia. If passed, the reforms will give the OAIC access to a broader range of enforcement options, as well as new functions and capabilities. These include provisions which allow for the appropriate tailoring of civil penalties to the level of seriousness of the breach, access to the general investigation and monitoring powers under the *Regulatory Powers (Standard Provisions) Act 2014* (Cth). The reforms will also enhance the powers of the Court in civil penalty proceedings beyond pecuniary penalties, to enable the making of any order in relation to the contravention;
- Enhanced privacy protections for children are looking likely to arrive in Australia in the next few years. Entities should have a clear understanding of what information they hold about children (likely to be defined as <18) so that they are ready for this change. There will likely be efficiencies for entities with global operations given the Australian Government's intent to align the COP Code with similar overseas children's codes, such as the UK's *Age Appropriate Design Code*.
- Several other reforms aimed at ensuring transparency and certainty regarding the handling of PI are also on the immediate horizon. If passed, these reforms will require entities to review and update their existing practices and policies to ensure compliance with the amended privacy laws. This will include updating their privacy policy to include information about any use of PI to make substantially automated decisions which could reasonably be expected to significantly affect the rights or interests of individuals;
- Significantly for defendants who might be subject to a claim following the occurrence of a data breach, the proposed statutory tort for serious invasions of privacy is actionable without proof of damage. While a plaintiff must prove that the relevant invasion was committed intentionally or recklessly, in a data breach context, the vulnerability leading to the breach may have been well known to the defendant or in the industry, potentially providing a basis for a finding of recklessness or imputed intent.

Data Breaches Up, So Protecting Yourself is Crucial, Says New OAIC Report

Authors: Brenton Steenkamp (Partner), **Utsab Banskota** (Manager) and **Deepa Thakkar** (Senior Manager) Clayton Utz

The latest Notifiable Data Breach Report from the OAIC (published 16 September) highlighted the significant rise, year on year, of data breaches affecting Australians, with increasingly severe and far-reaching impacts on personal data – and on the organisations affected by them.

The OAIC's Report provides not only guidance to the organisations affected by a data breach, but also recommended considerations that can play a role in protecting individual privacy whilst reducing the likelihood and impact of data breaches, thereby improving the cybersecurity posture and compliance with regulatory requirements.

Data breaches in Australia: the key takeaways from the OAIC Report

Data breaches are on the rise, with a 9% increase in data breach incidents this reporting period (January to June 2024) compared to the previous six months.

No sector is immune to data breaches, with both public and private entities being impacted, as evidenced in the OAIC's Report; but of those that reported data breaches:

- Continuing from the last reporting period, the Health sector remains the top sector affected by notifiable data breaches.
- Government agencies are experiencing increasing number of data breaches and have moved up from fifth place to second, with a 65% increase in notifiable data breaches compared to the last reporting period.
- The Education sector, which did not appear in the top five in the previous reporting period, is now among the top four sectors affected in Australia.

Cyber security incidents continue to remain as the top cause of data breaches, accounting for a total of 38% of the all the data breaches reported. These cannot all be blamed on technical deficiencies. The human element in protecting individual privacy and security cannot be stressed enough. Human error contributed to 30% of breaches, mostly involving misdirected emails and unauthorised disclosures.

The OAIC is adopting a risk-based and harm-focused approach in taking regulatory action in response to a data breach. To support that, the OAIC has the authority to conduct investigations, accept enforceable undertakings, and issue determinations to organisations as needed.

What can organisations do to improve their data protection?

One thing is clear from the OAIC Report, if it wasn't already: protecting individual privacy must be a top priority for organisations, not an afterthought.

That means you should recognise that individuals, clients, third-party stakeholders, and the OAIC expect a privacy-centric approach to be embedded in all aspects of their business operations, ensuring compliance with the privacy obligations.

In the next column are some actionable considerations:

Build tone from the top: Data breaches have the potential to impact individuals' privacy on a significantly large scale. As stated in the OAIC's Report, Medibank allegedly interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personal information. In an era where, on the one hand, organisations are collecting and processing large volumes of customer data and, on the other hand, there is an increasing number of sophisticated cyber-attacks, it is imperative for organisations' leadership teams to actively oversee their privacy practices and foster a culture of responsibility and accountability. This should start with organisations understanding the nature of their data holdings, including personal information holdings, and establishing "fit for purpose" privacy and security governance arrangements.

Implement robust security practices: Organisations must adopt robust cybersecurity practices and technologies to safeguard individuals' personal information against the evolving threat landscape. As highlighted in the OAIC's Report and supported by our experience, a "defence-in-depth" strategy should be employed, incorporating multiple layers of security measures throughout the organisation. This approach ensures that personal information remains protected even if a particular control fails. For organisations seeking to establish effective security measures to protect such information, the OAIC's Report recommends aligning their processes, policies, and administrative activities with cyber security standards and frameworks such as the ASD's Information Security Manual, NIST Cybersecurity Framework, ISO 27001/2, and ASD's Essential Eight.

Manage supply chain risks: Third-party suppliers are not just external entities, but integral parts of many organisations when it comes to the collection and management of the personal data they hold. Organisations must realise that while they could delegate their operational processes to these third-party suppliers, they cannot completely transfer their responsibilities for cyber security and privacy risks. In fact, from our experience, using a third-party supplier often introduces a heightened privacy risk which the organisation should carefully consider. Therefore, organisations must thoroughly evaluate the systems, processes, and procedures adopted by their third-party supplier in protecting personal information. Additionally, organisations should assess how these third-party suppliers manage privacy and security protection with their own downstream fourth- and fifth-party suppliers to ensure comprehensive privacy protection throughout the supply chain.

Train and educate staff at all levels: Employees across all levels of the organisation, should be aware of their privacy and security responsibilities. As suggested in the OAIC's Report; to mitigate the risk of human factor as a root cause of a data breach, organisations should educate their staff to reduce technical errors but also educate them to be aware of their privacy and security obligations. Additionally, organisations must consider the likelihood of an insider threat when developing these training and educational programs. From our experience, organisations generally focus on training their staff to protect individual privacy and security from external threats but tend to neglect that such threats could also present within their organisation.

Book Review

Rolph on Defamation 2nd Edition

By Professor D Rolph

Author: Justice Jacqueline Gleeson

In 2019, the New York Times declared Australia to be the defamation capital of the world. That feels right. Media reports of defamation proceedings in Australian courts are read and discussed voraciously. One defamation judge has been named by the AFR this week as the 5th most culturally aware and 5th most powerful lawyer in the country.

In contemporary Australia, defamation is a topic of general interest. Once upon a time, slanders were described as “mere wind”.¹ As a young defamation lawyer, I thought of defamation as tomorrow’s fish wrapper, such is the ingratitude of youth. But times have changed. With the proliferation of internet technologies, almost all of us are publishers and the prospect of being the subject of publications of adverse comment to an audience beyond our families is real.

And so, I commend to you the second ed of Rolph on Defamation. The 1st ed has been cited by superior courts across Australia, including by the High Court (in *Fairfax v Voller*) and by the eminent defamation judge mentioned earlier. The text will satisfy multiple audiences. For me, the early chapters on the competing interests in defamation law, reputation and freedom of speech, and the history of defamation law, were most interesting. They contextualise Prof Rolph’s treatment of the law, assisting us to understand what is at stake when we contemplate a legal problem that might involve defamation. I was interested to reflect on different aspects and concepts of reputation and heard a quiet lament from the Prof at the bottom of p 15: “A person might in fact have a reputation for being thin and beautiful but whether defamation law would ordinarily provide a remedy against disparagement of those aspects of appearance is open to doubt”. Prof Rolph discusses the interplay between defamation and protection of freedom of speech, including the important idea of the “chilling effect” of defamation laws, with special attention to the implied freedom of political communication.

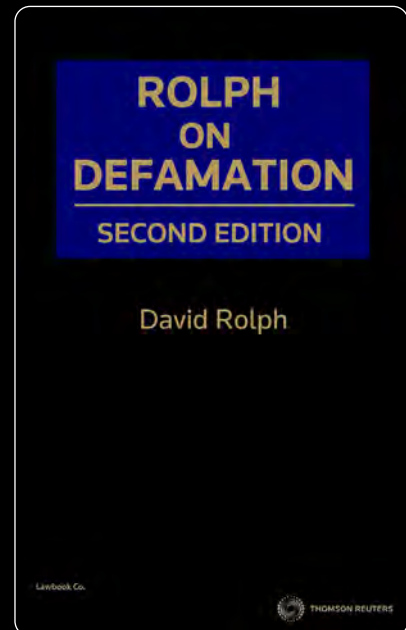
Chapter 3, on the history of defamation law, helps us to recognise the different concerns that have informed the development of the law over time which is often of importance when a novel case requires courts to think about where they should go next. This chapter also contains an explanation of the tortured history of defamation law reform.

In terms of jurisdiction, I was interested to read the Professor’s reflections on the emergence of the Federal Court as something of a magnet for defamation litigants. The Prof explains how the Federal Court has come to attract defamation jurisdiction and makes interesting and pointed remarks about the relationship between the so-called national, uniform defamation laws and the Federal Court, as well as the possible impact of the requirement for serious harm to establish liability under those laws upon the Federal Court as a venue for pure defamation actions.

As to substantive defamation law, I focused my attention on Ch 8, concerning publication and Ch 9, concerning the new requirement for serious harm to establish liability for defamation under the so-called national uniform defamation laws.

Publication is an issue of current significance, particularly because of the many questions arising out of the use of internet technologies to communicate defamatory material. I noticed, and read, Prof Rolph’s thoughtful and somewhat reproachful analysis of the High Court’s judgments in *Google v Defteros*. I regret to say that Rolph on Defamation was not cited in that case, and perhaps that is somehow relevant.

The analysis of *Google v Defteros* provides a good example of Prof Rolph’s willingness to point out areas for development of the law. More generally, this text does not simply teach the law. Rather, it helps the reader to understand the drivers of the law and to locate areas for legal disputation including, potentially questions for the grant of special leave to appeal. The enthusiastic litigant,



or their enthusiastic advocate, is encouraged to think creatively and deeply about their legal problem and its solution.

Although my early cynicism about defamation law has moderated, at least as a matter of principle, the requirement of proof of serious harm to reputation seems attractive. For practitioners, Prof Rolph provides a detailed consideration of the procedural rules governing determination of this element of the cause of action, which include powers, exercisable by the judge on their own motion, to determine this issue at an early stage. It is interesting to note that Prof Rolph has, appropriately, located case law from the NSW District Court and the Victorian County Court, to inform the reader about how to navigate the requirement of serious harm in a context where, it must be obvious, there can be a real prospect of the costs of litigation exceeding the hoped-for benefits to the grief of all concerned. This should be particularly useful for practitioners who do not practise exclusively in defamation law.

In conclusion, I congratulate Professor Rolph on his excellent scholarly contribution to the law of defamation in this country through the 2nd ed of Rolph on Defamation.

¹ See Rolph para 3.30



Interview with Jason Qian

Legal Counsel at TikTok

Author: Jeren Gul, Associate at Gadens and CLB editorial assistant

Jason Qian, Legal Counsel at TikTok in Sydney, is a solicitor whose career has always focused on media industry, especially in the digital space, and is currently in-house at the short-form video platform that has taken the world by storm. Since its launch only a few years ago, TikTok has established itself as one of the most popular entertainment platforms and, in 2021, was ranked the most popular website in the world. Prior to working at TikTok, Jason spent many years at Ashurst and at Simpsons, among other places where he honed his craft as a media, technology and IP lawyer, and has been a much-loved member of CAMLA throughout his career. **Jeren Gul**, Associate at Gadens and CLB editorial assistant, sits down with Jason to discuss his career and his thoughts about the industry.

JEREN GUL: Hi Jason, thanks so much for chatting with us about life as a TikTok lawyer. Let's jump right in! So: "Lawyer at TikTok". A dream role for many CLB readers and CAMLA members! Can you tell us what led you to your current gig?

JASON QIAN: Thanks for getting in touch! I had a very typical career path in some ways. After uni, I clerked at Ashurst (with a bunch of mootings and law society extra-curriculars on my CV) and settled in the IP/TMT team. After a few great years supporting some really interesting litigation and all the other bits and pieces that Ashurst offered, I decided I wanted to be more directly involved in the legal/creative space (whatever that meant), and moved to a very small boutique firm that mostly supported creative agencies and small businesses across a range of practice areas. I then found myself at Simpsons Solicitors until the TikTok role opened up, and thankfully my blend of big firm and boutique entertainment-related experience was what they were looking for. I can't remember exactly what I said in the TikTok interview, but I probably waxed on about getting legal rigour from Ashurst, and memorising contract negotiation playbooks and directly dealing with artists and clients at the boutiques.

JEREN: Aside from hours and hours of cool content creation (we assume), what's a typical day like for a lawyer at TikTok?

JASON: I wish there were hours and hours of cool content creation! I still leave that to the experts. But a typical day for me might involve:

- taking stock of the creator events that our team wants to draft contracts for, and figuring out what contracts we need in a conversation with the Procurement team;
- reviewing contract amendments from a headliner for our end-of-year TikTok

Awards show at the Hordern Pavilion;

- responding to my legal colleagues from Canada and Thailand about our standard operating procedures on certain on-platform issues;
- reviewing a recent case or piece of regulatory guidance to see whether we need to change how we do things or if any other teams should be informed; and
- meeting with the Tax team and Procurement team to talk about improving our procurement processes.

You know, there are a lot of atypical days. This week I've been going to SXSW, where I've been going to things like a panel with the eSafety Commissioner, a keynote by the CEO of Twitch about community and livestreaming, and sessions on every conceivable angle on AI in Australia, and I'll be reporting back to the team.

There's certainly less pure legal work than I was doing in private practice. I think there are some very smart lawyers (whom I deeply respect) who would prefer to get fed interesting problems and be kept as far away from the business people as possible. That's definitely not what my role involves! Everything we do is to support the business.

JEREN: Based on your experience, what skills or expertise do you think are essential for social media lawyers? Relatedly, what skills do you most value in your outside counsel and their advice?

JASON: You know, I wouldn't describe myself as a social media lawyer - TikTok is more of an entertainment platform and tech company. That said, understanding all the issues associated with massive amounts of user-generated content is a must.

It's a hard question because tech companies need all kinds of expertise, and

it can be split between team members in-house and outside counsel any which way. If you were a social-media focused lawyer I'd say internet advertising and communication expertise would be essential - think consumer law, platform liability, intellectual property particularly around images, video and music, specific advertising laws around various types of products like therapeutic goods, and content classification. And often an in-house lawyer's bread and butter involves commercial contracting (contract law and unfair contracts).

But you know, if your question is ultimately directed at the skills you need to work at a tech company in the social media or entertainment space, there are many roads to it. You could be an employment lawyer, or pure IP / trade marks lawyer, or a litigator dealing with disputes, or a lawyer working in the payments space, or a corporate lawyer helping the company with major transactions. A big tech / social media / entertainment company might need any of them.

Anyway, the legal expertise and skills (which you can honestly just google) are table stakes. What really differentiates social media / tech lawyers is their understanding of the products, events and industry they're working on, and the people they're working for. Do you know why people livestream on Twitch and TikTok, and how important it is as a source of community for some groups? Do you know what (non-legal) incentives are involved in creators disclosing or not disclosing brand partnerships? How easy is it to definitively find out who controls the music that the artist you're contracting with has written? What is the industry-standard email marketing platform, and does it help you comply with the Spam Act?

My business stakeholders aren't evaluating me based on whether my answer is

technically legally correct. They assume so, and evaluate me based on whether I get them and their struggles, and give them a response that helps them (and here, a clear no is better than a longwinded maybe). And that's not just my business stakeholders but also my cross-functional teams, like my tax and procurement and government relations colleagues.

It's the same response for what I'm looking for in outside counsel – understanding the business, the product, and the stakeholders. And being concise. It's so critical but sadly, often overlooked. I really feel this sense of moral injury receiving advices in Word which waste the first page listing assumptions and background and take forever to get to the point.

JEREN: How does your team keep up to date in such a rapidly evolving legal landscapes?

JASON: Any way we can! Digesting law firm updates, reading juicy cases as they come down. Critical things like

the Online Safety Act we naturally are reading every update and standard as they come through. As a team we do try to think about what, pragmatically, needs to change in response to a given legal change (and often the answer is that our existing processes or documents already cover it). Oh, and CAMLA! I'm a huge fan of CAMLA events and the *Communications Law Bulletin* (the International Women's Day editions are so impressive), and I tell everyone in the office to become a member.

JEREN: Obviously! Finally (and most importantly), tell us about some of your favourite TikTok accounts.

JASON: That's a great question, thank you for asking!

I actually really like my TikTok feed. I'm digging some of the trends - #BookTok got me onto Madeline Miller's *The Song of Achilles*, a beautiful retelling of the Iliad from the perspective of Patroclus, #GymTok's helping me puzzle out hip anatomy as my body fails me, and I get a lot of what are essentially positive

woo-woo affirmations in my feed which I roll my eyes at but probably contribute positively to my mental health.

Specific accounts? I like @dexter.mp4, who shares videos where he talks about eclectic things, like why there are so many types of plankton or the Simpsons Paradox, this statistics phenomenon where a trend that appears in data can appear to reverse itself when looking at subsets of that data. @gee_derrick is a thoughtful Australian commentator on all things music. @zachwoods (who plays Gabe on The Office and Jared from Silicon Valley) posts truly unhinged skits, like a track where he berates you for staying awake in a decreasingly relaxing ASMR whisper.

JEREN: Brilliant – I'll have to check them out! Thanks so much Jason. On behalf of all our readers, we're really grateful for your insights!

JASON: Thank you for having me, and look forward to the next CAMLA event!

Event Report: CAMLA Cup

Author: Alana Callus, Associate at the Federal Court of Australia and CAMLA YLC Member

Move aside ARIA Awards - the 2024 CAMLA Cup was the night of nights for Australian media and communications lawyers. The annual trivia extravaganza, held this year on 5 September at Sky Phoenix, was hosted by the dynamic duo, **Sylvia Alcarraz** and **Nick Kraegen**, supported by a team of the CAMLA Young Lawyers, who brought their illustrious expertise and quick wit to the evening.

As always, each team gathered around lazy susans to challenge their pop culture prowess and test their legal literacy

in fast-paced rounds in an effort to be declared CAMLA Cup champions. There was a healthy dose of camaraderie and competition between law firms and in-house teams alike, but there could only be one winner. After several years of settling for second place, the **Gilbert + Tobin** team were finally triumphant and claimed the coveted CAMLA Cup for 2024.

Thank you to all the volunteers who worked behind the scenes to make this annual event a success, diligently judging the results and delivering the well-

deserved prizes. On behalf of CAMLA, we would also like to extend a special thanks to each team for creating a fresh set of media-related puns for their team names and generously donating prizes (all eyes were on the Haigh's giant frogs). Looking forward to seeing everyone again next year!



Game Over, or a Glitch?

The Potential Copyright Concerns with Integrating AI-Generated Assets in Video Games

Author: Sol Bedi (Lawyer) Cam Rogers Legal

Introduction

Since the introduction of the Digital Games Tax Offset and the reintroduction of game development funding programs (grants) by the Australian Government in 2023, video game development in Australia is arguably at an all-time high.¹ One of the latest advancements in game development is the use of artificial intelligence tools and learning-language models (“AI”) to assist in the development process. With a demand for interactive games reaching peak levels in Australia,² the utilisation of AI in game development can significantly reduce development timelines and hard costs (e.g., programmer and artist fees), allowing developers to ship their titles much more quickly than ever. The aim of this article is to consider whether Australian video game developers can integrate AI-generated assets into their games lawfully, with a particular focus on the issue of copyright infringement. When considering AI in the context of game development, it is crucial to separate the situations where AI is utilised into two distinct categories.³ The first category being the player experience, i.e., AI being used to deliver real-time feedback or interactive elements to end-users, and the second being using AI in the development process.⁴ This article solely considers the latter and, more specifically, examines the issues associated with integrating AI-generated assets into games through a copyright lens. It concludes with a review of some of the practical considerations legal practitioners should consider when advising clients, from an industry perspective.

Copyright Challenges

For an AI-generative application (“AI-application”) to generate a “new” image or asset, it must first be trained on data to both comprehend end-user instructions and also enable it to respond to those inputs. Generative AI-applications are trained on algorithms. The nature of these algorithms include machine learning frameworks and architecture, such as diffusion models and generative adversarial neural networks. These then teach the underlying AI a range of behaviours, including, to identify patterns across images and make judgements, ultimately allowing it to respond to an input, namely, generating an asset. Subsequently, as AI is trained upon data such as images and artwork, there are several copyright challenges (and issues) associated with AI-applications, and subsequently, AI-generated assets. These challenges exist across two lenses, one from the input lens (i.e., the data the

AI-application is trained upon) and two, from the output lens (i.e., the AI-generated asset). They are interrelated, as the output of an AI-application depends on its input. This article focusses on the output of AI, and more importantly, the issue of copyright infringement arising from the creation and commercial use of AI-generated assets.

However, it is important to highlight that the issue of infringement is not an isolated one. Other copyright challenges such as authorship, originality and moral rights also exist. That being said, as the issue of copyright infringement poses greater risk to video game developers, this article contemplates infringement, the implications of infringement for developers, and considerations legal practitioners should make.

Copyright Infringement

The issue of copyright infringement in this context rests upon two points: (1) whether the data and materials that an AI-application has been trained upon to deliver an output are protected by copyright; and (2) whether the proprietor of the AI-application has the necessary rights to draw upon said copyright protected material to train the AI. Given the use of AI in game development primarily concerns the creation of in-game ‘assets’, the notion of ‘artistic works’ frames the following discussion of infringement.

In the context of generating assets for video games, various AI-applications can generate in-game artistic works such as characters, images, maps, environments and other related assets by drawing from numerous pre-existing artistic works and photographs, within their dataset(s). Subsequently, it becomes apparent that AI-applications, specifically their underlying language models and algorithms, may infringe copyright if the AI has been trained upon material that is protected by copyright. Consequently, it is entirely possible for AI-generated assets to reproduce, adapt and exploit works protected by copyright in full, or more commonly, in part. The question then becomes, does the creation of an AI-generated asset in this context constitute copyright infringement in Australia?

Under the *Copyright Act 1968* (Cth),⁵ the threshold for copyright infringement is that a ‘substantial part’ of a ‘work’ must be reproduced or communicated for infringement to occur.⁶ Jurisprudence informs us that the measurement of what constitutes a ‘substantial part’ must be conducted in

1 Australian Government (Cth), *Revive, Australia’s Culture Policy for the next five years* (2023), 86.

2 Jeffery Brand, IGEA, *Australia Plays 2023* (Annual Report, 2023) 3.

3 David Zeffman, ‘AI-ming high: the integration of AI into gaming’ (2023) *CMS Law-Now*, 1, 1-2.

4 *Ibid.*

5 *Copyright Act 1968* (Cth) (‘Copyright Act’).

6 *Copyright Act* (n 5), s 14(1).

a qualitative manner and not quantitatively,⁷ and that such analysis is a question of fact and degree.⁸ Consequently, unless an AI-generated asset is substantially similar in appearance to a pre-existing artistic work, such as reproducing the same watermarks like in the matter of *Getty Images v Stability*,⁹ the AI-generated asset is unlikely to infringe pre-existing works. However, there might be an argument that if a “small part” of a work which requires a high degree of skill to create has been reproduced (or communicated) in a AI-generated asset, it may be regarded as ‘substantial’ and therefore constitute copyright infringement.¹⁰ Although a difficult argument to substantiate, such argument could be supported by reference to the fact that AI-applications are trained upon diffusion models and neural networks which enable them to meaningfully respond to end-user inputs. Therefore, such ‘responses’ involve a high degree of skill (artificial in this case) when reproducing, manipulating and exploiting existing materials to produce a newly generated asset.

In contrast, it may be argued that the creation of an AI-generated asset constitutes copyright infringement on the basis that the proprietor of the AI-application (or the end-user) has performed an act, such as reproducing an ‘artistic work’ in a material form, without the necessary license (i.e., consent).¹¹ However, this argument will ultimately rest upon whether a court finds that the defined term of ‘material form’ extends to include the exploitation and adaptation of pre-existing artistic works by the AI-application in one of two situations.¹² The first being the development of the underlying AI itself (i.e., the training of the AI, via neural networks and diffusion models) and the second being the creation of the AI-generated asset as a result of the end-user inputs and instructions. Consequently, when considering whether the creation of an AI-generated asset constitutes copyright infringement, the question is ultimately fact dependent, calling for the need of judicial consideration.

Although there is no authoritative jurisprudence supporting the position that the creation of AI-generated assets constitutes copyright infringement in Australia, reference should be made to the ongoing matter of United States case *Andersen et al v Stability AI Ltd. et al.*¹³ In *Andersen*, the plaintiffs have alleged that numerous AI-applications have trained upon (and still draw from) data that is protected by copyright, without the requisite licenses, and that such conduct constitutes copyright infringement.¹⁴ Recently, the United States District Court for the Northern District of California denied the defendant’s motions to dismiss

these allegations and will proceed to hear the allegations of copyright infringement. Further, in jurisdictions such as Germany, commentators such as *Dimov*¹⁵ argue that AI-generated content which has been derived from copyright protected material may constitute a ‘reproduction’ under Section 16 of Germany’s copyright laws (*UrhG*).¹⁶ Subsequently, there is a possibility that if an AI-application has been trained upon, or is drawing upon, material that is protected by copyright without the proprietor of the AI-application having the necessary rights to do so, then that AI-generated work (and/or its later exploitation by developers) may infringe upon third-party copyright.

Defences to Infringement

Given the requirement for use to be ‘fair’, it is unlikely that any of the exceptions within the scope of ‘fair dealing’ could be successfully argued by developers due to the underlying commercial nature (and intention) of integrating AI-generated assets in games. While other jurisdictions such as the United States have the defence of ‘fair use’ and the United Kingdom has the text and data mining exception, Australian developers do not have the benefit of these defences. Subsequently, the only potential defence that Australian developers may have could exist within Section 43A of the Copyright Act (temporary reproductions). Using that section of the Act, a developer could argue that the response from an AI-application (i.e., the ‘output’) constitutes a “communication” for the purposes of said provision.¹⁷

Responsibility for the Infringement

If an argument for infringement is successful in Australia, the question then remains, who is liable for the infringement? Is it the developer who uses the AI platform, the publisher of the developer’s game, the proprietor of the AI-application, or a combination? Although no legal proceedings have commenced in Australia for copyright infringement against owners or users of AI systems, several concerns have been raised.¹⁸ Recent litigation in the United States indicates that liability is more likely to rest with the proprietors of AI-applications, rather than end-users. However, to answer this question properly, the copyright issues of ‘authorship’, ‘ownership’ and ‘originality’ need to be addressed.

Perhaps an argument could be formed that end-users could be liable in the event they are found to be ‘authors’ of their AI-generated assets? Although unlikely given current litigation, this view might be supported in Australia given

7 *Milpurruru v Indofurn Pty Ltd* [1994] FCA 1544 209.

8 *IceTV v Nine Network Australia* 254 ALR 386, 395.

9 *Getty Image s(US), Inc. v. Stability AI, Inc.*, 1:23-cv-00135-JLH

10 *Blackie & Sons Ltd v Lothian Book Publishing CO Pty Ltd* (1921) 29 CLR 396.

11 *Copyright Act* (n 5), s 31(1).

12 *Copyright Act* (n 5), s 10.

13 *Anderson et al. v Stability AI Ltd. et al.* (United States District Court and Northern District of California San Francisco Division, 3:23-cv-00021, 01/01/2023).

14 *Ibid.*

15 Vitorio Dimov, ‘AI Content in Gaming: What About Copyright?’ (2023) *Härtling*.

16 *Gesetz über Urheberrecht und verwandte Schutzrechte* (Germany) 1 March 2018, *UrhG*, 2018, 16.

17 *Copyright Act* (n 5).

18 Attorney-General’s Department (Cth), *Third roundtable on Copyright*, High Level Summary September 2023.

the High Court's decision in *Data Access Corp v Powerflex Services*. That case held that a human who employs 'skill' and 'judgment' during the creation process of computer-generated data can be afforded copyright protection.¹⁹ However, only time will tell whether an end-user can be afforded authorship over AI-generated assets in Australia and ultimately, who bears the legal responsibility if such assets do constitute copyright infringement.

Considerations for Legal Practitioners and their Clients

When acting for game developers, legal practitioners should be mindful of not only the copyright challenges associated with integrating AI-generated assets into video games, but also other related legal implications. Two examples include making warranties under third-party agreements and challenges preventing digital distribution.

Third-Party Agreements

Legal Practitioners need to be aware of the types of warranties that developers are likely to make (or have made) under government funding agreements and third-party publishing agreements. Under these types of agreements, developers routinely warrant and represent that the underlying rights of their video game do not infringe the rights of any other third-party, and/or that the underlying rights of their game are "original". Moreover, both Government screen agencies and third-party publishers require developers to warrant that they either own, or have the exclusive rights to, all underlying rights in their game(s). In some instances, third-party publishers may require a developer to make a 'blanket warranty' that their game does not feature any AI-generated assets. Subsequently, the integration of AI-generated assets into the development process of a game is likely to have a material impact on the types of warranties that developers can make under these agreements.

While the Federal Government screen agency (Screen Australia) recently published their 'AI Guiding Principles' indicating that screen practitioners may use AI during their development processes, this does not negate developer obligations (or contractual promises) under relevant grant (or funding) agreements. Subsequently, practitioners should engage in meaningful consultation with both screen agencies and third-party publishers, to ensure that developers are able to integrate AI-generated assets within development, in a lawful manner. To provide informed and effective advice in such scenarios, practitioners should carefully review the end-user licence agreements relating to the AI-applications that their client/s intend to utilise in development to ensure that (a): the data that the AI-application is trained upon, and drawing from, is not protected by copyright, (b): the developer has the necessary rights to commercially exploit AI-generated assets into their game and (c): whether the AI-application indemnifies the end-user (and their affiliates) from claims relating to copyright infringement.

Distribution

In a situation where an AI-application only grants end-users a *non-exclusive* licence to use generative works and/or does not allow for commercial use of said assets, practitioners should be aware of the challenges relating to distribution. If a developer integrates an AI-generated asset into their game but does not have the *exclusive* right to commercially exploit such asset, this may prevent the developer from acquiring a third-party publisher (due to the warranties that they need to make in those arrangements), ultimately forcing them to 'self-publish'. While the barriers to self-publishing are very low, a developer in such situation is likely to find their ability to commercially distribute their game on digital platforms and storefronts is restricted.

Practitioners also need to be aware that some digital distribution platforms will reject games that utilise, or integrate, AI-generated artwork. For example, it was recently reported and confirmed that Valve, the operator of the platform Steam, rejected a developer's video game from being available on Steam. This was because Valve discovered the game featured artistic works that were generated by AI which had been derived from copyrighted material.²⁰ In light of this, Valve then updated its 'submission guidelines' outlining that developers may not publish content that they "don't own or have the adequate rights to" on Steam.²¹ Valve also updated its Distribution Agreement to include a 'AI Content on Steam' policy. That policy explicitly prohibits the use of "illegal or infringing content" in games published on Steam, as well as an obligation for developers to disclose the use of AI-generated assets.²²

Consequently, given these legal and practical challenges to distribution, practitioners should caution developers when it comes to integrating AI-generated assets (which are created, or derived, from material protected by copyright) into their games. Doing so may expose them to claims of copyright infringement, or a breach of third-party agreements, especially if they intend to commercially exploit their video games.

Conclusion

When considering whether Australian developers can incorporate AI-generated assets into their video games, the question comes down to whether the data used to train the AI-application is protected by copyright and if so, whether the proprietor of the AI-application has the necessary rights to exploit that material accordingly. However, even if a proprietor has the necessary rights to train the underlying AI of their applications, practitioners need to be aware that developers still require the rights to commercially exploit AI-generated assets in their video games, and that there may be contractual challenges relating to digital distribution. Although there has yet to be any successful litigation relating to copyright infringement in this context, this should not lull developers (or their legal representatives) into comfort, as copyright infringement is not the only legal issue at play.

19 *Data Access Corporation v Powerflex Services Pty Ltd* [1999] HCA 49.

20 Paul Tassi, 'Steam is Reportedly Rejecting Games Using AI Art', *Forbes* (online, 29 June 2023) <<https://www.forbes.com/sites/paultassi/2023/06/29/steam-is-reportedly-rejecting-games-using-ai-art/?sh=e563fc42a7e8>>; Devin Coldeway, 'Valve responds to claims it has banned AI-generated games from Steam', *TechCrunch* (online, 4 July 2023) <<https://techcrunch.com/2023/07/03/valve-responds-to-claims-it-has-banned-ai-generated-games-from-steam/>>.

21 Steam, 'Steam Distribution Agreement', *Steam Direct* (Web Page) <<https://partner.steamgames.com/steamdirect>>.

22 *Ibid*.

Birkenstock Shows That it is Possible to Secure Trade Mark Protection Over the Shape of Popular Product Designs

Authors: James Neil (Partner) and **Connie Beswick** (Senior Associate), Clayton Utz

Stopping others from copying your product designs is a perennial problem, particularly for those in the fashion industry. In Australia, protection for the design of products such as footwear is normally obtained through the registered designs system. However, Birkenstock is seeking to protect its footwear designs using trade mark registrations. This article examines how Birkenstock can protect its popular shoe designs using shape trade mark registrations and why trade mark protection over its designs might be preferred over other forms of IP protection.

Birkenstock's shape trade marks

The Australian Trade Marks Office (ATMO) has recently published a decision by which several Birkenstock shape trade marks were accepted for possible registration.

Birkenstock already had a trade mark registration for its iconic "Arizona" sandal shape as shown below:



In this recent decision, Birkenstock has also now achieved acceptance for some of its other popular styles shown below:



The "Gizeh"

The "Madrid"

The "Mayari"

The "Boston"

How did Birkenstock obtain trade mark protection over the "shape" of shoes?

Trade mark applications – whether they be for words, logos, shapes or anything else – will be rejected if they are not capable of distinguishing the goods or services of one trader from the similar goods or services of another. In essence, this is determined by asking whether the trade mark is something which other traders are likely to want to use on or in connection with their similar goods.

As you might expect, many shape trade mark applications are met with a distinctiveness objection, such as on the basis that the application claims footwear and the trade mark is in the shape of a shoe which other traders would want to use – including due to its functional aspects. In order to achieve acceptance, brand owners then need to file evidence of their extensive use of the trade mark to demonstrate that consumers have, in fact, come to associate the shape with their particular business, despite the lack of inherent distinctiveness.

In Birkenstock's case, the ATMO was willing to grant acceptance over these shape trade marks because, despite having a functional aspect, the shapes of the shoes were somewhat distinctive. Notable features included:

- a wide footbed and thick outer and inner sole, creating a "chunky" aesthetic;
- the thickness of the straps adding to the "chunky" appearance;
- large square buckles on the straps;
- a moulded sole which included toe bars, footbed rims and heel cups;
- a "squiggly" grid pattern on the outer sole; and
- the silhouette or outline of the footwear.

There was also evidence of long-time use, significant promotion, celebrity endorsement, and the manner in which the marks were used. This included the fact that footwear is typically sold in stores displaying the goods so consumers are exposed to the footwear itself (and are not, for instance, immediately exposed to an accompanying word trade mark).

Birkenstock also applied to register the shapes of its “Florida” and “Zurich” styles, but was not successful due to the low levels of sales of those styles.

Trade mark versus design protection

Birkenstock’s case highlights the potential for trade mark law to be used as a tool by brand owners (and their licensees) to stop third parties from copying their valuable product designs and maintain exclusivity in the market.

In Australia, there are many different types of “signs” which can be registered as a trade mark, including words, logos, colours, sounds, scents and “shapes”. Usually, the scope of protection over the “shape” will be defined by the shape as depicted in representations or images attached to the trade mark application form, which will appear on the Trade Marks Register.

While shape trade marks are not as common as word or logo trade marks, there are currently 1,255 registered shape trade marks on the Australian Trade Marks Register. There are a number of footwear shape trade marks that are registered, owned by companies such as Crocs, Superga and R. M.

Williams. Examples of other registered shape trade marks relate to the shape of beverage and perfume bottles, bags, toys, chocolate, biscuits, pens and vehicles.

It is generally very difficult to secure registration of a shape trade mark. However, Birkenstock’s case shows that it is very much possible to do so where sufficient evidence is available.

Applying for a design registration can be an easier and less costly option. Designs can provide exclusivity in relation to one or more visual features of a product. Their validity is not assessed by reference to any “distinctiveness” test, but merely need to be new and distinctive compared with what has gone before.

However, a drawback of registered designs is that they only provide protection for a maximum of 10 years. Trade mark protection is a better option in that respect as trade mark registrations can be renewed indefinitely. For example, Weber Barbeques owns shape trade mark registrations which are still valid and enforceable, despite having been filed almost 30 years ago.

Overall, when seeking to protect their product designs, brand owners and designers have a number of different options available. However, Birkenstock’s recent success shows that shape trade mark registrations should be considered in appropriate cases, and can be a very effective way to stop copycats in their tracks.

The CAMLA Board for 2024

President: Rebecca Dunn, Gilbert + Tobin

Vice Presidents

Debra Richards, Netflix

Martyn Taylor, Norton Rose Fulbright

Treasurer / Public Officer: Julie Cheeseman, Bird & Bird

Secretary: Marlia Saunders, Thomson Geer

CLB Editors

Eli Fisher, Paramount

Ashleigh Fehrenbach, RPC

Committee Members

Sylvia Alcarraz, Dentons

Chris Chow, Creative Lawyers

Gillian Clyde, Creative Lawyers

Emma Johnsen, Marque Lawyers

Nicholas Kraegen, Baker McKenzie

Rebecca Lindhout, HWL Ebsworth

Tess Mierendorff, Herbert Smith Freehills

Marina Olsen, Gadens

Nicholas Perkins, Ashurst

Shanna Protic Dib, MinterEllison

Katherine Sessions, Office of the eSafety Commissioner

Calli Tshipidis, Foxtel

Jade Tyrell, Johnson Winter Slattery

Tim Webb, Clayton Utz



CAMLA Young Lawyers for 2024

Chair: Belyndy Rowe, NBCUniversal

Vice Chair: Erin Mifsud, ITV (UK)

Secretary: Kathy Janevska, Canva

Committee Members

Lucy Hughes, Stan

Laksha Prasad, Marque Lawyers

Dan Roe, Disney

Imogen Loxton, Ashurst

Justin Kardi, Sky News Australia

Alana Callus, Federal Court of Australia

Isabella Barrett, Corrs Chambers Westgarth

Kristina Hewetson, Baker McKenzie

Tara Hayes, ABC

Maddie Merchant, BBC

Matthew Salgo, The Wiggles

Lewis Graham, Allens

Jeren Gul, Gadens

Daniella Lambert, MinterEllison



Annual Oration

2024

TO BE DELIVERED BY

THE HON JUSTICE MICHAEL LEE

Contemporary Challenges with Open Justice

THURSDAY | **14** | NOVEMBER

ASHURST BALLROOM, 5 MARTIN PL,
SYDNEY NSW 2000

Time: 6:00 pm, Keynote address at 6:30pm
followed by a cocktail reception

Attire: Semi-formal

Price: \$100 CAMLA members
\$120 non-members

REGISTRATIONS OPEN AT
WWW.CAMLA.ORG.AU/SEMINARS

ENQUIRIES: CONTACT@CAMLA.ORG.AU

Ashurst

Legislation Introduced to Combat Mis- and Dis-information on Online Platforms

Authors: Justine Munsie (Partner) and **Brodie Campbell** (Senior Associate), Addisons

The *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024* (Cth) (the **Bill**) was introduced into the House of Representatives on 12 September 2024. The Bill is not intended to cover the dissemination of all types of false content, but rather the dissemination of content that is verifiably false, misleading or deceptive and which causes or contributes to serious harm.

The Bill has three main objectives:

- to empower the federal media regulator, the Australian Communications and Media Authority (**ACMA**), to require digital communications platform providers to take steps to manage the risks posed by misinformation and disinformation online;
- to increase transparency regarding the way in which digital communications platform providers manage misinformation and disinformation; and
- to empower users of digital communications platforms to identify and respond to misinformation and disinformation online.

The Bill does not empower the ACMA to take down individual content or user accounts but is rather targeted at the development and enforcement of industry codes and standards.

What is the reason for the changes?

In February 2021, the Australian Code of Practice on Disinformation and Misinformation (the **Code**) was released by DIGI, a not-for-profit industry association representing the digital platform industry. The Code, which is opt-in, is overseen by the ACMA and requires signatories to commit to a number of measures to address the spread of misinformation and disinformation on their platforms.

There are currently only nine signatories to the Code: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok, Twitch and Legitimate. X (formerly Twitter) was a signatory to the Code until its signatory status was withdrawn in November 2023.

In its June 2021 and June 2023 reports to the Australian Government regarding the operation of the Code, the ACMA noted that there were a number of shortcomings in the self-regulatory arrangement. The Bill has

therefore been designed to enhance and complement the framework under the Code and to incentivise digital communications platform providers to have robust systems and measures in place to address misinformation and disinformation online.

A draft version of the Bill was released last year for public consultation.

Who does the Bill apply to?

Under the Bill, the proposed laws will apply to “digital communications platform providers”. “Digital communications platforms” are defined to include:

- connective media services, being services that enable online interaction between two or more end-users;
- content aggregation services, being services that collate and present content from a range of online sources to end-users;
- media sharing services, being services that provide audio, visual (animated or otherwise) or audio-visual content to end-users;
- internet search engine services; and
- other kinds of digital services determined by the Minister for Communications from time to time.

Internet carriage services, SMS services and MMS services are excluded from the definition of “digital communications platform”.

What does the Bill require digital communications platform providers to do?

The Bill requires digital communications platform providers to increase their transparency with Australian users about how misinformation and disinformation is handled on their services. Specifically, the Bill requires that digital communications platform providers:

- assess risks relating to misinformation and disinformation on their platform and publish the results of that assessment;
- publish policies in relation to the management of misinformation and disinformation; and
- publish media literacy plans setting out the measures that they will take to ensure that end-users are better able to identify misinformation and disinformation.

¹ The approach under the Bill relating to the development of disallowable enforceable industry codes is similar to the position taken under Australia’s online safety regime. For more information, see our previous Insight [Online Content Regulation in Australia](#)

The Bill enables the ACMA to approve and register enforceable misinformation codes that have been developed by the digital platform industry (**Misinformation Codes**). If the ACMA considers that the industry misinformation codes are not adequate, the ACMA may determine misinformation standards for sections of the digital platforms industry (**Misinformation Standards**).¹

The Bill also enables the ACMA to make rules requiring digital communications platform providers and implement a complaints and dispute resolution process regarding online misinformation and disinformation.

Failure to publish required information or to make information available to the ACMA when requested, as well as non-compliance with a Misinformation Code or Misinformation Standard more generally, is punishable by the ACMA. The enforcement mechanisms available to the ACMA include the issue of formal warnings, remedial directions or infringement notices, as well as commencing proceedings seeking the imposition of civil penalties and/or injunctions. Civil penalties are severe and can range up to the greater of 25,000 penalty units (currently \$7,825,000) or 5% of annual turnover for some contraventions.

What types of content does the Bill apply to?

The Bill sets a high threshold for the types of content that would be considered to be misinformation or disinformation. Broadly speaking, in order for the prohibitions under the Bill to apply, the content must be:

- reasonably verifiable as false, misleading or deceptive; and
- reasonably likely to cause or contribute to “serious harm”.

The types of “serious harms” covered by the Bill include:

- harm to the operation or integrity of an electoral or referendum process in Australia;
- harm to public health in Australia including to the efficacy of preventive health measures;

- vilification of a group in Australian society on the grounds of race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin, or an individual because of a belief that the individual is a member of such a group;
- intentionally inflicted physical injury to an individual in Australia;
- imminent damage to critical infrastructure or disruption of emergency services in Australia; and
- imminent harm to the Australian economy.

Whether content would be considered to be misinformation or disinformation is dependent on the intention of the person who engages in the dissemination of the content – if there are grounds to suspect that the person disseminated the content with the intention to deceive others, the content would be considered disinformation; if there is no such identifiable intention, the content would be misinformation.

Importantly, the Bill does not apply to the dissemination of:

- content that would reasonably be regarded as parody or satire;
- professional news content (ie. content disseminated by persons or organisations who produce and publish online news content and who are subject to professional rules and editorial standards); or
- content for any academic, artistic, scientific or religious purpose (provided that the dissemination is reasonable).

What’s next?

The Bill is currently in the early stages and is before the House of Representatives. The Bill is yet to be voted on.

The most vocal criticism about the Bill, and the consultation draft release last year, was the potential for the proposed changes to limit free speech. It is expected that there will be significant debate about whether the Bill has struck the correct balance.

We will be monitoring the progress of the Bill closely.



Boost

Your CAMLA Corporate Membership

Why limit your CAMLA corporate membership to just 5 members?

Add your colleagues for only \$60 per person per year so they too receive the many benefits of CAMLA membership including an annual subscription to the *Communications Law Bulletin* and discounts on CAMLA seminars.

If you’d like to take advantage of this great offer, Please contact Katie Walker at: contact@camla.org.au

Australian “Social Media” Age Restrictions May Be on the Way with South Australia Championing Reform

Authors: Sophie Dawson (Partner) and **Hamish Lennon** (Associate), Johnson Winter Slattery

On 8 September 2024, the Honourable Robert French AC released the ‘Report of the Independent Legal Examination into Banning Children’s Access to Social Media’ (**French Review**) which includes a consultation exposure draft of the *Children (Social Media Safety) Bill 2024 (SA)* (**draft Bill**) for the Premier of South Australia.

The French Review details an indicative legislative model which includes a duty of care for social media services to prevent access to “social media services” by children in South Australia under the age of 14 and by 14- and 15-year-old children who do not have parental consent. Any breach of the duty gives rise to a cause of action for which damages are available as a remedy. An infringement notice can also be issued resulting in payment of a penalty.

Potential for federal intervention

On 10 September 2024, in an interview with ABC News Breakfast, Prime Minister Anthony Albanese commented on the proposed draft South Australian reforms. The Prime Minister stated that the Federal Government will consider both the recommendations of the French Review and the proposed draft Bill to inform the design of “a national response, rather than eight different state responses.” The Prime Minister also confirmed that the Federal Government is consulting on introducing a social media age limit between 14- and 16-years of age and that federal legislation will be introduced in Parliament by the end of this year.

On 10-11 October 2024, the South Australian and New South Wales State Governments ran a Social Media Summit (**the Summit**) which focussed on the design and delivery of reform to address regulatory challenges posed by social media. Minister for Communications, Hon Michelle Rowland MP, addressed the Summit setting out that the Federal Government’s approach for reform would include:

- **Exemptions:** the creation of exemptions which incentivise platforms to develop “age-appropriate versions” of services that protect children by design.
- **Timeline:** a 12-month implementation timeline to allow industry to establish systems for compliance.
- **Social responsibility:** an overarching strategic objective that “social media must exercise a social responsibility” with reform placing the onus on platforms to protect children from online harms.
- **Regulatory alignment:** broader alignment with the existing regulatory landscape and the findings of the independent review of the *Online Safety Act 2021 (Cth)* (**OSA**), which is due to be released on 31 October 2024.

The Minister for Communications also stated that while consensus on the ‘right’ age for age limits is unlikely and that digitally savvy young people will find ways to circumvent controls, it’s the Federal Government’s position to not to let ‘perfect’ be the enemy of good and to “signal a set of normative values” around protecting children online.

At the Summit, eSafety Commissioner, Julie Inman-Grant, shared the statistic that nationally 84% of Australian children aged 8-12 have used social media and messaging services since the beginning of 2024. The eSafety Commissioner also flagged that the proposed age limit may drive conversations regarding online harms between young people and trusted adults underground and drive savvy young people towards under-regulated “darker recesses of the internet”.¹ The eSafety Commissioner also highlighted the importance of online social platforms for certain cohorts (including LGBTQI+ teens, First Nations teens and those with disabilities) who have built supportive connections and communities online.

It’s important to note that if the Federal Government were to legislate in this area, Commonwealth legislation would prevail over State legislation to the extent of any inconsistency and will exclude the operation of State legislation if the Commonwealth legislation covers the field.

Scope of the proposed reforms – defining ‘social media services’

The proposed scope for the South Australian draft Bill’s application is ‘social media services’, the proposed definition of which is based on the definition from the OSA. However, the draft Bill adopts a slightly modified definition to also capture electronic services with instant messaging functionality, discussion forums, content sharing features, livestreaming platforms and other online video games.

The draft Bill also provides a definition for ‘exempt social media service(s)’ which includes services that are designated by a notice as exempt or a service that is a member of a class of social media services designated as exempt by the Minister. The French Review proposes ‘EdTech applications with social functions’ as a potential class of exempt social media services, notable examples in this proposed class include YouTube, Roblox and Minecraft. From notes in the French Review regarding consultation between Google and Justice French, it appears YouTube has been suggested as an exempt service as it does not recommend content based on user interaction or other social connections. YouTube also provides a dedicated ‘YouTube Kids’ service.

¹ eSafety Commissioner, *Learning from the past to safeguard children’s online future* (10 October 2024).

² eSafety Commissioner, eSafety submission to the *Joint Select Committee on Social Media and Australian Society* (21 June 2024) 11.

The French Review considered five other proposed definitions for ‘social media services’, each of which are variations of the definition contained in the OSA. Some of these proposed variations on the definition expressly include or exclude messaging services, online multiplayer video games, internet search engines and app distribution services. As such, the proposed scope of reform seemingly extends well beyond traditional conceptions of ‘social media services’ and the reform will instead broadly capture most services that enable any form of online interaction between users.

The eSafety Commissioner has previously warned of the difficulties associated with trying to separate ‘social media’ from “the rest of the internet and modern media”, stating that “even if social media could be demarcated and separated from other media, a primary concern is that children would migrate to other services and platforms with fewer safeguards.”²² The eSafety Commissioner has also flagged that restricting young people from ‘social media’ may limit some from having “access to critical support” and encourage others to work around any limits.

Summary of key draft provisions

The legislative model set out in the draft Bill includes the following proposed reforms:

| Reform focus | Proposed changes |
|------------------------|---|
| Regulator | A new South Australian Regulator of Child Social Media Safety (Regulator). |
| Duty of care | A new duty of care on: <ul style="list-style-type: none"> non-exempt providers of social media services to prevent access to that service in SA by any South Australian child: (i) under 14; and (ii) aged 15 or under, unless consent is received from the child’s parents; and all providers of social media services to take all reasonable steps to prevent access to that service in SA by any South Australian child: (i) under 14; and (ii) aged 15 or under, unless consent is received from the child’s parents. <i>(as above, an ‘exempt social media service’ means a service designated by notice as exempt or a service which is a member of a class of social media services designated by the Minister (e.g. ‘EdTech applications with social functions’))</i> |
| Defence | A defence is available for a non-exempt provider of social media services if it can prove, at the time of the breach, it had taken all reasonable steps to prevent access to its social media services. <i>(measures that constitute ‘reasonable steps’ are to be prescribed by regulations under the Bill)</i> |
| Enforcement mechanisms | The reforms provide for a range of enforcement mechanisms, including: <ul style="list-style-type: none"> infringement notices – issuable by the Regulator where there are reasonable grounds to believe a social media service has contravened a duty of care; compensation and civil penalty orders – the Supreme Court of SA, where satisfied a duty of care has been breached on the balance of probabilities, may make orders for: (i) compensation; and (ii) civil penalties (where the breach of duty was wilful, reckless or repeated); and other available Court orders – including declarations, injunctions and civil damages (in the context of the direct right of action, discussed below). <i>(provisions specifying amounts payable for infringement notices / compensation orders / civil penalties are to be fixed by regulations under the Bill. Any amount paid under the Bill will be paid into a ‘Children’s Online Safety Fund’ (Fund) established by the Bill, and the Regulator may apply the Fund towards: (i) enforcement costs; (ii) research costs; (iii) discretionary payments to children who have suffered harm; and (iv) community educational efforts.)</i> |
| Cause of action | The proposed reforms also provide that where a social media service provider breaches the duty of care and a child (under 16-years of age) suffers mental or physical harm as a result of access contrary to the duty of care, the breach of duty of care will be actionable as a tort by the child (or the child’s parent, or the Regulator in its discretion) and damages may be awarded against the provider as if the breach of duty of care constituted negligence by the provider. |
| Complaints mechanism | A complaints mechanism that allows individuals to complain on behalf of children to the Regulator where a South Australian child is being provided with access to a non-exempt social media service, contrary to the service’s duty of care. |

The proposed definition of ‘social media services’ captured by the draft Bill is set out below:

social media service means –

- (a) *an electronic service that satisfies 1 or more of the following conditions:*
- (i) *the sole or primary purpose of the service is to enable online social interaction between 2 or more users;*
 - (ii) *the service allows users to link to or interact, or interact with, some or all of the other users;*
 - (iii) *the service allows users to post material on the service;*
 - (iv) *the service is a relevant electronic service;*
 - (v) *the service satisfied any other conditions prescribed by the regulations; or*
- (b) *a service, or service of a class, prescribed by the regulations; but does not include an exempt social media service. In determining what the sole or primary purpose of a service is for the purposes of paragraph (a)(i) of the definition of social media service in subsection (1), the purposes of advertising, or generating revenue from advertising are to be disregarded.*

Next steps

In light of the above developments, businesses that fall within the broad ambit of “social media service” providers will need to keep an eye out for future iterations of the draft Bill, particularly once before the South Australian parliament, and for other broader Federal and State level reform / consultation processes in this space.

“Consent or Pay” Models Under Scrutiny in UK and EU

Authors: Olly Bray (Partner) and **Ashleigh Fehrenbach** (Senior Associate), RPC

The question: Are “consent or pay” business models compliant with EU and UK data protection law?

The key takeaway

The European Data Protection Board (EDPB) has issued an opinion stating that, in most cases, it will not be possible for “large online platforms” to comply with the requirements for valid consent under the EU GDPR if they confront users only with a binary choice between consenting to the processing of personal data for personalised advertising and paying a fee.

In the UK, the Information Commissioner (ICO) has initiated a (now closed) consultation on “consent or pay” business models, the responses to which will contribute to the ICO’s upcoming guidance on cookies and similar technologies. In an initial view accompanying the consultation, the ICO indicated that access mechanisms are not likely to comply with expectations in data protection law for consent to be “freely given” where they do not provide people with a free choice about whether to receive personalised ads.

The background

“Consent or pay” refers to the choice given to users by some service providers so they can either access online services without payment if they consent to their personal data being used for personalised advertising or pay to access those services without personalised advertising. This model has been the subject of increasing debate globally.

On 17 April 2024, the EDPB released an opinion in response to requests from the Dutch, Norwegian and German Supervisory Authorities addressing the circumstances under which “large online platforms” can implement consent or pay models in a manner that constitutes valid, freely given consent under the EU GDPR. The EU GDPR does not define “large online platforms” but the EDPB suggests this could be understood as including “very large online platforms” as defined under the EU Digital Services Act and “gatekeepers” as defined under the EU Digital Markets Act.

Separately, on 6 March 2024 the ICO called for views on the use of “consent or pay” business models more broadly. This consultation closed on 17 April 2024.

The EDPB’s view

The key points from the EDPB’s opinion were that:

- consent or pay models will only be valid if providers can demonstrate that consent from the user is informed, unambiguous, specific and freely given;
- the CJEU confirmed in the Bundeskartellamt judgment that users who refuse to consent to particular processing operations should be offered, “if necessary for an appropriate fee, an equivalent alternative not accompanied by such processing operations”;
- however, personal data should not be treated as a tradeable commodity, and only offering a paid alternative to a service which includes processing for behavioural advertising purposes should not be the default for large online platforms. Large online platforms should instead assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances, considering possible alternatives to personalised advertising

that entail the processing of less personal data as well as the balance of power between data subjects and the provider;

- consent will not be freely given if data subjects cannot refuse or withdraw consent without detriment, and detriment may arise where (i) non-consenting data subjects who do not pay the fee face exclusion from the service, and (ii) the fee imposed effectively inhibits data subjects from making a free choice; and
- large online platforms should therefore consider providing data subjects with an “equivalent alternative” that does not entail the payment of a fee eg with a form of advertising involving the processing of less (or no) personal data. In most cases, whether a further alternative without behavioural advertising is offered by the large online platform, free of charge, will have a substantial impact on the assessment of the validity of consent, in particular with regard to the detriment aspect.

In most cases, it will not be possible for large online platforms to comply with the requirements for valid consent under the EU GDPR if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

The ICO’s view

The ICO’s position on consent or pay business models will become clearer once its upcoming guidance on cookies and similar technologies is published, however the ICO’s initial view suggests that it will take a similar approach to the EDPB. Some key takeaways from the ICO’s initial view are:

- in principle, data protection law does not prohibit “consent or pay” models. However, any organisation considering such a model must be careful to ensure that consent to the processing of personal information for personalised advertising has been freely given, is fully informed and is capable of being withdrawn without detriment; and
- the ICO recommends that businesses consider several factors when assessing if their consent or pay model constitutes valid consent under the UK GDPR, namely, the power balance between the business and users, the equivalence between the paid-for and free services, whether the fee is appropriate, and whether the choice to users is presented fairly and equally.

Why is this important?

Personalised advertising is lucrative, much more so than non-personalised advertising. Digital businesses that deploy a consent or pay model have typically done so in order to recoup revenue lost by users refusing to consent to personalised advertising. Although the EDPB and ICO do not prohibit the use of consent or pay models entirely, both regulators view consent obtained in this way as a lawful means of processing personal data in only a limited number of tightly defined scenarios, and not an approach that should be widely adopted as default. As a result, we may see companies that have typically generated revenue from personalised advertising, or consent or pay, needing to find new ways of funding their services.

Any practical tips?

Large online platform providers that operate consent or pay models in the EU, need to consider whether their existing practices are likely to give rise to consent from users that is

informed, unambiguous, specific and freely given. If not, they should consider whether any changes can be made to their existing practices (eg offering a free “equivalent alternative”) or whether the model is appropriate at all. The EDPB has also indicated that it plans to issue connected guidance on the use of consent or pay models by all providers operating in the EU (ie not just large online platforms), and so other providers that operate consent or pay models in the EU need to be equally mindful that changes are on the horizon.

Similarly, all providers operating consent or pay models in the UK should look out for the ICO’s forthcoming guidance on cookies and similar technologies. In light of the ICO’s initial

view, they might also consider whether the consent they are getting is likely to be considered informed, freely given and capable of being withdrawn without detriment.

Australian regulators are yet to publicly opine on consent or pay models by large online platform providers. That being said, the ACCC has taken an active regulatory role in the digital platform services space over the past few years, most recently in its ongoing 5-year Digital Platform Service Inquiry. Whilst the final report of that inquiry won’t be delivered to the Treasurer until 31 March 2025, early indications suggest that Australia’s regulatory approach will converge with what has been adopted in the EU and UK.



COMMUNICATIONS AND MEDIA LAW ASSOCIATION
END OF YEAR DRINKS
THURSDAY 5TH DECEMBER
6-8PM
GILBERT + TOBIN
LEVEL 35, 200 BARANGAROO AVE
SYDNEY

RSVP BY THURSDAY 31 NOVEMBER VIA
WWW.CAMLA.ORG.AU/SEMINARS



Top of the Menu: ACMA Puts Free-to-air in the Spotlight with New TV Prominence Framework

Authors: Timothy Webb (Partner), **Joel Parsons** (Senior Associate) and **Chelsea Manansala** (Lawyer), Clayton Utz

Key Takeaway

The Australian Communications and Media Authority (**ACMA**) has released a public consultation paper inviting feedback on the new TV prominence framework. Designed to ensure that free-to-air services and apps are easily accessible on smart TVs, this framework aims to prioritise Australian broadcasters in an increasingly crowded digital space.

The ACMA has released a **public consultation** paper seeking views on implementing Australia's new TV prominence framework.

Feedback and evidence from the consultation will help to determine if, and how, the ACMA uses its powers to oversee and enforce the TV prominence framework. Submissions to the ACMA closed on 15 October 2024..

Background

In July 2024, the Australian Government passed legislation that established a prominence framework for certain internet connected television devices (**regulated television devices**), such as smart televisions and smart media streaming devices, to ensure that Australians will be able to easily find and readily access broadcasting video on demand (**BVOD**) and linear broadcast services (together, **regulated television services**).¹ Regulated television services include broadcast services provided by Seven, Nine, Ten, the ABC and SBS, and their corresponding BVOD services: 7plus, 9Now, 10play, ABC iView and SBS on Demand.

The framework will apply to all regulated television devices manufactured and supplied in Australia on or after 10 January 2026. As part of the new changes, the ACMA has been provided with powers to oversee and enforce the TV prominence framework, including the power to:

- make guidelines about regulated television devices, including determining whether a specified device is, or is not, a regulated television device;
- describe or determine requirements for a primary user interface on regulated television devices; and
- determine the circumstances in which a regulated television service is offered, including determining different circumstances for different regulated television services.

These changes emerge as a result of fundamental transitions which have occurred in the television content market over the last decade, both in Australia and overseas. The market has shifted towards on-demand services, and audiences now have the ability to select specific applications to access content on-demand, introducing a new level of competition where Australian broadcasters must compete with international content providers. In this evolving landscape,

smart TVs and other regulated television devices act as the gateways for users to access these services.

The new TV prominence framework therefore aims to ensure that local broadcast and free-to-air services are given sufficient 'prominence' or visibility on the main user interface of regulated television devices. By establishing minimum prominence standards, the framework is intended to guarantee that Australian audiences can easily access local free-to-air television content on connected television devices in Australia amidst the growing array of digital and on-demand services.

Key issues for consultation

Defining a regulated television service

One of the key issues on which the ACMA is seeking feedback as part of its public consultation concerns which devices are to fall within the scope of "regulated television device". Only such devices will be subject to the minimum prominence requirements under the TV prominence framework.

Subsection 130ZZI(1) of the *Broadcasting Services Act 1992* (Cth) (**BSA**) defines a regulated television device as domestic reception equipment that:

- i. is capable of connecting to the internet and providing access to broadcasting video on demand services; and
- ii. is designed for the primary purpose of facilitating the viewing of audiovisual content.

In addition, the BSA provides that if required, the ACMA may determine whether a specified domestic reception equipment is, or is not, a regulated television device.

The ACMA's preliminary view is that, consistent with the "primary purpose" test in subsection 130ZZI(1) of the BSA, smart televisions and smart media streaming devices (for example, Google Chromecast, Apple TV, Fetch TV, Hubbl and Amazon Fire TV Stick) will be considered regulated television devices under the TV prominence framework, whereas mobile phones, tablets, laptops, desk computers and video game consoles will *not* be considered to fall within the definition. This is because although these devices may have the purpose of facilitating the viewing of audiovisual content as one of their purposes, this is not their *primary* purpose, and those devices would not therefore meet the primary purpose test.

¹ See the *Communications Legislation Amendment (Prominence and Anti-siphoning) Act 2024* (Cth), which made various amendments to the *Broadcasting Services Act 1992* (Cth) and the *Australian Communications and Media Authority Act 2005* (Cth).

This view is in contrast to some stakeholder views which have argued for a more expansive scope, and that certain devices such as mobile phones, laptops and tablets should be included. Smart monitors and smart projectors have also been considered as potentially falling within the definition, and the ACMA regards these as “edge” cases which will require greater consideration on a case-by-case basis. Moreover, as manufacturers respond to customer demands which evolve over time, the ACMA prefaces that its guidance about regulated television devices may also change.

As part of its consultation, the ACMA is specifically seeking comment on this key issue in relation to:

- views on the proposed considerations that the ACMA should take into account when applying the primary purpose test; and
- whether further clarification is needed on whether certain devices are, or are not, a regulated television device.

Defining a primary user interface

Another key issue that the ACMA is considering as part of its consultation is in relation to the meaning of the “primary user interface” of a regulated television device. Under the TV prominence framework, all regulated television services will be required to be displayed on a device’s primary user interface.

Section 130ZZL of the BSA provides that the primary user interface of a regulated television device means the interface of the device that:

- (a) is either or both of:
- (i) the home screen or main screen of the device; and/or
 - (ii) the main interface most commonly used to provide access to applications that make audiovisual content available on demand using a listed carriage service; and
- (b) meets the description or requirements (if any) determined by the ACMA.

The ACMA’s preliminary view is that technical or contractual obstacles may prevent manufacturers from being able to display all regulated television services on its home screen without needing to scroll. It is therefore proposed that the primary user interface should be described as a virtual space that may extend beyond the bounds of the screen. However, scrolling to reach all regulated television services should not extend indefinitely – specifically, the ACMA considers that scrolling to reach all regulated television service applications should not go beyond a space that is double the initial view.

For example, on a user interface which displays 8 icons on the initial view, all regulated applications would be required to appear within the first 16 tiles that are displayed to the user (being the 8 original icons on the initial view, and the further 8 icons that appear upon scrolling). For vertical scrolling interfaces, the ACMA has indicated that all regulated television service apps should be displayed within the first 2 ribbons or rows, and for a grid interface in which scrolling has the effect of moving between different ‘pages’, all regulated television services should be required to be displayed within the first 2 pages.

The ACMA is aware that some devices use a content aggregating interface, which does not display a scrollable list of applications on the home screen but rather displays icons of audiovisual content from across different subscription and broadcasting television services that are personalised to the

user (such as by recommending titles from across different applications which are all of a particular genre). The ACMA also regards the variety of devices and operating systems, and the risk of changing market dynamics or interfering with contractual arrangements, as relevant considerations.

The ACMA was therefore seeking comment on the following specific areas:

- whether the ACMA should exercise its discretion to set specific descriptions or requirements for a device’s primary user interface, and if so, if this should include scrolling;
- whether ribbon or row layouts require different consideration to grid layouts;
- whether content aggregating interfaces should be treated differently from other regulated television devices when describing primary user interface requirements; and
- whether existing contracts between device manufacturers and content providers (e.g., streaming services) limit the ability to provide prominence to Australian broadcaster apps (BVOD) on the primary user interface.

As part of its consultation, the ACMA was also seeking evidence of images of smart TV and streaming device home screens to help the ACMA understand how BVOD and subscription video on demand (SVOD) apps are positioned across different brands, with particular interest in major manufacturers like Samsung, LG and Sony, which dominate the Australian market.

Other issues for consultation

A key requirement under the TV prominence framework is that manufacturers must not supply a regulated television device in Australia if it does not comply with the minimum prominence requirements for a regulated television service that is ‘offered’ by a regulated television service provider. Manufacturers may therefore require clarity as to when a regulated television service is no longer offered by the regulated television service provider (i.e. an app is discontinued by the service provider), or in circumstances where a new application is being offered, the lead time required by manufacturers to incorporate these new applications into the primary user interface.

To assist its consideration of these issues, the ACMA was also seeking feedback on:

- whether the ACMA should define what it means for a regulated television service to be “offered” and whether the ordinary meaning is sufficient;
- whether there is sufficient transparency around which apps are currently offered to manufacturers;
- what circumstances might justify a manufacturer rejecting an app; and
- whether different types of regulated television services require different considerations regarding the offering or rejection of apps.

The ACMA is also seeking evidence of the following:

- information on which platforms and operating systems support regulated television services;
- how app developers ensure that their apps are compatible with different devices or operating systems, including any internal or external certification processes;

- the required timelines for incorporating new regulated television service apps into devices, and when manufacturers consider an app too late to be pre-installed or added during setup; and
- data on the costs involved for both regulated television service providers when offering apps to manufacturers and for manufacturers in assessing or accepting these apps, including indicative figures on these expenses.

Key takeaways

The new TV prominence framework is particularly relevant for those in the TV industry including traditional free-to-air broadcasting networks, streaming services, and television and device manufacturers. Related industries such as advertising agencies, media companies and telecommunications providers are also likely to be interested in these changes due to its implications for audience viewership and engagement, advertising revenue and data consumption. The new framework will also directly affect how individual consumers access and interact with television content on smart TVs and similar devices.



Ashurst

The Future of Australian Content (Part III): Recent legislative developments - Anti-Siphoning and Prominence

Please join us for the latest instalment of our Australian content seminar series where we will look at recent developments in the content regulation space and be joined by industry experts to discuss the impacts of the changes to the anti-siphoning regime and new smart device prominence requirements.

Panellists:



Bridget Fair
Chief Executive Officer
Free TV Australia



James Grant Hay
Executive Director
CTVMA

Chaired by Nick Perkins (Ashurst) and Calli Tshipidis (Fox Sports)

Wednesday, 30 October | 6-7 PM followed by networking drinks

Chatham House Rules apply

Ashurst, Level 11, 5 Martin Place, Sydney NSW 2000

CAMLA members: \$65 | non-members: \$95

Registration: www.camla.org.au/seminars

Enquiries: contact@camla.org.au

Event Report: CAMLA Young Lawyers Committee - Media, Law & The Games Seminar

Author: Tara Hayes (Lawyer) Australian Broadcasting Corporation and CAMLA YLC Member



With the closing ceremonies of the Paris 2024 Games, the Olympics and Paralympics have wrapped up for another four years, with Australian athletes returning home with a swag of medals including 18 gold at both events. There is a minefield of legal and regulatory considerations to ensure major sporting competitions of this kind are fair and that fans across the globe can follow the action every step of the way.

On August 13, the CAMLA Young Lawyers Committee hosted an in-person seminar at Marque Lawyers in Sydney with the topical and insightful discussion featuring Calli Tspidis (Foxtel Group), Hannah McLean (Bird & Bird), Richard Burgess (Football Australia) and Tim Fuller (Dentons). The panel was moderated by CAMLA YLC members, Lucy Hughes (Stan) and Justin Kardi (News Corp Australia).

The seminar kicked off with a discussion of the role that intellectual property rights and legislation plays in protecting Olympic and Paralympic materials, including the iconic symbols. The panel also covered the allocation of media rights and navigation of Media Access Rules (including the 3 x 3 rule) for coverage rollout across various platforms, as well as specific rules in the Olympic Charter relating to advertisement and sponsorship. The rationale behind these restrictions, practical implications for stakeholders, guidance and enforcement avenues were discussed, as well as similar protections in other sporting contexts.

The panel then dove into a conversation on the structure and processes involved in the regulation and governance of sport and the main matters impacting stakeholders at both professional and grassroots levels. Sports integrity issues including doping, eligibility and selection were dissected with the panel drawing on recent controversies to illustrate the key concerns, processes, disciplinary procedures and related media coverage.

On behalf of CAMLA, the CAMLA YLC would like to thank all the panellists for sharing their expertise and the attendees for joining the educational and engaging discussion. We would also like to thank Marque Lawyers for hosting this in-person event.



Responsible Use of AI: New Australian Guardrails Released

Authors: Sonja Read (Partner), **Shane Evans** (Partner), **Chelsea Gordon** (Senior Associate), **Sam Burrett** (AI Lead), MinterEllison

We explore the Australian Government's two newly released publications to guide the development and deployment of AI in Australia.

The Australian Government has released two publications to guide the development and deployment of artificial intelligence (AI) in Australia: the "Proposed Guardrails for the Mandatory Use of AI in High-Risk Settings" (**Proposals Paper**) and the "Voluntary AI Safety Standard" (**Standard**). These publications clarify the Government's intention for AI regulation in Australia and offer guidance for organisations seeking to implement responsible AI practices.

The proposed guardrails and voluntary standard mark a significant step on the journey to AI regulation in Australia. These measures are designed to complement existing legal frameworks, including privacy, consumer protection, and corporate governance laws. In addition, both the Standard and the Proposals Paper align the Australian Government with international developments in AI regulation, particularly in Canada, the US, and the EU.

For organisations developing or deploying AI, it is essential to stay across these and future regulatory developments, and to proactively adopt responsible AI practices. This will enable organisations to effectively mitigate regulatory and operational risk, enhance stakeholder trust, and navigate the evolving regulatory landscape with confidence.

In this article, we outline the key features of these publications, examine the differences between them, and contextualise this announcement from the Government in Australia's evolving landscape of AI Regulation and Governance.

Proposed Guardrails for High-Risk AI

The Proposed Guardrails outline 10 proposed mandatory guardrails for developers and deployers of AI systems in high-risk settings. These guardrails focus on ensuring testing, transparency, and accountability, to manage potential risks associated with AI systems.

Key aspects of the proposed guardrails include:

1. Establishing clear accountability processes, governance, and strategies for regulatory compliance
2. Implementing risk management processes to identify and mitigate risks
3. Protecting AI systems and data quality through governance measures
4. Testing AI models and systems before deployment and ongoing monitoring
5. Enabling meaningful human oversight and intervention in AI systems
6. Informing end-users about AI-enabled decisions, interactions, and AI-generated content

Key Takeaways

- The Australian Government has proposed 10 mandatory guardrails for high-risk AI as part of the ongoing consultations on safe and responsible AI.
- The Voluntary AI Safety Standard provides practical guidance on responsible AI implementation, broadly aligning with the proposed guardrails and international standards.
- Australian organisations should familiarise themselves with the proposed guardrails and start aligning their practices with the voluntary guidelines to prepare for forthcoming regulation.

7. Establishing processes for people impacted by AI systems to challenge outcomes
8. Ensuring transparency across the AI supply chain to effectively address risks
9. Maintaining records to allow third-party compliance assessments
10. Conducting conformity assessments to demonstrate compliance with the guardrails

The Proposals Paper also includes principles for determining high-risk AI settings and includes a definition of General-Purpose AI (GPAI) models. Feedback is sought on whether mandatory guardrails should apply to all GPAI models, or a subset based on risk indicators.

The Proposals Paper defines GPAI as:

"An AI model that is capable of being used, or capable of being adapted for use, for a variety of purposes, both for direct use as well as for integration in other systems."

This definition focuses on the versatility and adaptability of GPAI models, which can be applied to a wide range of use cases and integrated into various systems, unlike narrow AI models designed for specific tasks.

The Proposals Paper outlines the following principles for determining high-risk AI settings:

- a) Risk of adverse impacts on individual rights recognised under Australian and international human rights law,
- b) Risk of adverse impacts on an individual's physical or mental health or safety,
- c) Risk of adverse legal effects, defamation, or similarly significant effects on an individual,

- d) Risk of adverse impacts on groups of individuals or collective rights of cultural groups,
- e) Risk of adverse impacts on the broader Australian economy, society, environment, and rule of law,
- f) Severity and extent of the adverse impacts outlined in principles (a) to (e).

These principles consider the potential for AI systems to cause harm to individuals, groups, and society as a whole, taking into account factors such as human rights, health and safety, legal implications, and the severity and extent of adverse impacts.

These proposed guardrails are part of an ongoing consultation process, with submissions closing in October. If approved, it is anticipated that the regulations may not come into effect until 2025, allowing time for refinement based on the consultation process – and for Australian organisations to prepare.

Complementing existing requirements under legislation

The proposed mandatory guardrails for AI are designed to work in conjunction with existing legal frameworks that impact the development and use of AI in Australia. While the guardrails introduce new preventative measures, they do not replace or exempt Australian organisations from their obligations under current legislation. We highlight below some key areas where the guardrails complement existing laws.

Guardrail 2: Establish and implement a risk management process to identify and mitigate risks

Existing Laws / Regulation: This guardrail aligns with directors' duties under the Corporations Act 2001, which require directors to exercise powers and discharge duties with due care and diligence, and to assess and govern risks to the organisation, including non-financial risks such as those arising from AI and data.

Guardrail 3: Protect AI systems, and implement data governance measures to manage data quality and provenance

Existing Laws / Regulation: This guardrail is intended to complement requirements under other legislation, such as:

- the Privacy Act 1988, which places obligations on organisations handling personal information,
- the Copyright Act 1968, which gives owners of certain material exclusive economic rights that include the right to copy and the right to communicate the material to the public, and
- the Security of Critical Infrastructure Act 2018, which imposes security obligations on data storage and processing assets.

Guardrail 6: Inform end-users regarding AI-enabled decisions, interactions with AI and AI-generated content

Existing Laws / Regulation: This guardrail intersects with proposed reforms to the Privacy Act 1988 to enhance transparency about the use of personal information in automated decisions which have a legal or similarly significant effect on individuals' rights. It also complements prohibitions against misleading and deceptive conduct under the Australian Consumer Law.

Guardrail 7: Establish processes for people impacted by AI systems to challenge use or outcomes

Existing Laws / Regulation: Obligations under this guardrail will need to work alongside existing avenues for complaints handling, including rights and obligations under the Australian Consumer Law and administrative law.

Guardrail 8: Be transparent with other organisations across the AI supply chain about data, models and systems to help them effectively address risks

Existing Laws / Regulation: This guardrail aligns with requirements under privacy laws, intellectual property laws, duties of confidence and contract law which protect the use, reproduction and/or disclosure of data and AI models or systems without the requisite consents or rights.

Voluntary AI Safety Standard

Alongside the Proposals Paper, the Government released the Standard to provide guidance about responsible AI implementation. These Standards will operate while the regulations are being developed.

This Standard provides practical guidelines for organisations aiming to implement responsible AI practices. The Standards align closely with the proposed guardrails set out in the Proposals Paper, except for one key difference: the tenth guideline focuses stakeholder engagement over conformity assessments. Conformity assessments are being prepared for in the voluntary guardrails through several voluntary steps, including around record keeping, transparency and testing.

The Standard also provides guidance about AI procurement processes, to help organisations align their contracts (with suppliers and developers) with the Standards.

Notably the Standard aligns with international standards, particularly AS ISO/IEC 42001:2023 and NIST AI RMF 1.0. It thus promotes consistency and interoperability.

Implications for Australian organisations

These publications clarify the government's intent for AI regulation in Australia. The broad alignment with international approaches should create a largely standardised basis from which organisations invested in the use or development of AI can operate with confidence.

While the mandatory guardrails are still subject to consultation and refinement, organisations can start preparing by familiarising themselves with the proposed requirements and assessing their current AI practices. This should include pre-configuration considerations, such as appropriate data governance, privacy, and cyber security considerations to ensure a responsible and secure technology environment for the integration of AI.

In the interim, the Standard offers a practical and applicable framework for organisations to follow. By aligning their AI development and deployment practices with the voluntary guidelines, organisations can demonstrate their commitment to responsible AI and position themselves for a smoother transition once the mandatory regulations come into effect.

The Proposed Scams Framework: A Whole of Ecosystem Approach to Protecting Australians from Scams

Authors: Antonia Garling (Partner), **Silvana Wood** (Partner) and **Jeremy Jose** (Partner) G+T

On 13 September 2024, Treasury launched a consultation on Australia's proposed new scams prevention framework (**Scams Framework**). The Federal Government has pushed for this new framework in light of the significant increase in scam activity, evidenced by the fact that Australians lost \$2.74 billion to scammers in 2023.

In this article, we detail the proposed requirements of the Scams Framework in the exposure draft of the Treasury Laws Amendment Bill 2024: Scams Framework (**Bill**) and the explanatory materials as well as discuss the implications of the new framework for banks, telecommunications companies and digital platforms service providers.

This Bill, if passed, will establish a new whole-of-ecosystem approach containing specific 'principles-based' legal requirements for addressing scams and liability for breaching these principles.

Summary of the framework

The Scams Framework introduces mandatory requirements to combat scams and would primarily be inserted into law via a new Part IVF into the Competition and Consumer Act 2010 (Cth) (**CCA**).

The Scams Framework is part of a broader effort to modernise Australia's laws for the digital age and has the following key features:

- Overarching principles (governance, preventing, detecting, reporting, disrupting and responding to scams) that apply to regulated entities.
- Sector-specific codes that set out minimum standards for what each regulated entity in a sector must do to address scam activity on their regulated service and protect consumers.
- External dispute resolution schemes to provide consumers redress (including compensation) where regulated entities have not met their framework obligations.
- Enforcement by the Australian Competition and Consumer Commission (**ACCC**) and its delegates including for contravention of civil penalties includes fines of up to \$50 million, enforcement tools such as infringement notices, enforceable undertakings, adverse publicity orders as well as a private right of action for damages.

The Bill provides that the Treasury Minister will be empowered to designate a sector as being subject to the Scams Framework to respond to scam activity in the economy.

Alongside the launch of the consultation, the minister has stated that he will initially delegate the following as being subject to the Scams Framework:

- Banks
- Telecommunication service providers
- Digital platform services relating to social media, paid search engine advertising and direct messaging services.

Crypto asset platforms, superannuation firms and online marketplaces are not included (yet) in the list of regulated entities despite their involvement in the scams ecosystem.

The minister has also stated that it is the government's intention to designate the Australian Financial Complaints Authority (**AFCA**) as the sole external dispute resolution (**EDR**) scheme for the first three designated sectors.

The Scams Framework does not contain a mandatory reimbursement model of the kind about to go-live in October in the UK. Under the UK model, UK banks will be required to reimburse consumers up to a maximum of \$166,000 unless the consumer acted with gross negligence. Instead, Australian consumers will be able to obtain compensation via the AFCA or by exercising their private right of action for damages against regulated firms where they can establish a breach of the relevant legal requirements.

The ACCC will be the Scams Framework general regulator with responsibility for overseeing all regulated sectors to support an ecosystem wide approach. The ACCC's powers include monitoring and supervising compliance with the Scams Framework as well as undertaking investigations and enforcement for breaches. The ACCC will also be able to delegate its powers to other sector-specific regulators (for example, the Australian Securities and Investments Commission (**ASIC**) for the banking sector).

First legislative definition of a 'scam'

The Bill contains Australia's first legislative definition of a scam:

'A scam is a direct or indirect attempt to engage a consumer of a regulated service that: (a) involves deception; and (b) would, if successful, cause loss or harm including obtaining personal information of, or a benefit (such as a financial benefit) from, the consumer or the consumer's associates.'

According to the explanatory materials, this definition is deliberately broad to capture the wide range of activities scammers engage in and their ability to adapt to evolving behaviours over time. The concept of a 'benefit' includes non-monetary benefits and assets, such as cryptocurrency

or loyalty and rewards points. A consumer's associates include their relative, spouse, child, a partner of a partnership or a trustee of a trust.

Importantly, the definition covers 'attempts' to scam. An attempt involves deception if the attempt:

- Deceptively represents something to be (or to be related to) the regulated service.
- Deceptively impersonates a regulated entity in connection with the regulated service.
- Is an attempt to deceive the consumer into facilitating an action using the regulated service.
- Is an attempt to deceive the consumer that is made using the regulated service.

This broad definition crosses over significantly with existing legal concepts such as misleading or deceptive conduct as defined in Schedule 2 of the CCA.

Overarching principles

Subject to any amendments made to the final form of the Bill, all regulated entities will be required to comply with the six Scams Framework overarching principles, being: Governance, Prevent, Detect, Report, Disrupt and Respond. Compliance will be monitored and investigated by the ACCC as the general regulator.

A number of the principles require regulated entities to take 'reasonable steps'. 'Reasonable steps' are not defined in the Bill but should be objectively determined taking into account factors like the size, services, consumer base and types of scam risk relevant to the regulated entity.

Banks are already taking a range of steps in complying with the Scam Safe Accord, such as the introduction of confirmation of payee and sharing scam intelligence via the Australian Financial Crimes Exchange.

Sector specific codes

The Treasury Minister (or their delegate, which may include the ACCC, ASIC or a sector-specific minister or regulator) is empowered to make sector-specific codes by legislative instrument. These codes are intended to ensure that there is robust and targeted action in each sector, recognising the different positions that banking, telecommunications and digital platforms play in the scams ecosystem.

The sector codes must be consistent with the overarching principles (excluding reporting which will be covered in the CCA) but may also cover ancillary or incidental matters relevant to the particular sector. Obligations in the sector codes represent only minimum standards for what each regulated entity in a sector must do to address scam activity and protect consumers.

While the banking code is yet to be developed, the explanatory materials include examples of what could be covered in the banking code. Examples of banking code obligations may include:

- Governance: requirements for policies, procedures, metrics and targets which banks must have in place.

- Prevent: requirement to implement at least one biometric check for all individual consumers opening a new bank account.
- Detect: requirement to develop processes to flag, slow down or pause higher risk transactions that appear out of character for a particular consumer, such as large amounts of money being transferred to a new payee or into a cryptocurrency.

Further potential wording of a future banking code is listed in the first Treasury consultation.

Compliance with the code is monitored, investigated and enforced by the relevant sector regulator (ASIC for the banking code).

External dispute resolution

The minister intends to authorise the existing AFCA scheme as the EDR scheme under the Scams Framework. While complaints relating to banks are already covered by AFCA, the Scams Framework will enable consumers to also complain and seek compensation from banks, telecommunication companies and digital platforms service providers under the AFCA scheme.

It is anticipated that existing caps on the amount of compensation available under the AFCA scheme will apply under the Scams Framework. The current maximum a consumer may claim is capped at \$1.2 million.

Welcoming the Treasury consultation, AFCA stated that in 2023-24 it received approximately 11,000 scam-related complaints. AFCA Chief Executive, David Lock, said that businesses "should not wait until they are required by codes to take action but should now take all actions possible to prevent, detect and disrupt scams".

Consumers can already raise a complaint to AFCA about scams associated with their bank. While the Government has said that the EDR scheme "will provide victims with a clear pathway for redress", it remains unclear at this stage how the EDR scheme will improve on the existing EDR process.

Consequences for breach

The ACCC (as general regulator) together with sector-specific regulators will be empowered to conduct investigations into possible contraventions of the principles and codes. The principles and codes are civil penalty provisions, breaches of which will result in liability for a civil penalty.

The Bill divides civil penalty provisions into tier 1 contraventions (being contraventions of the principles to prevent, detect, disrupt and respond to scams) and tier 2 contraventions (being breaches of a code or the principles relating to governance and reporting).

The civil penalty regime is supported by a range of other administrative enforcement tools as alternatives to litigation. These include powers to impose infringement notices, enforceable undertakings, seek injunctions, issue public warning notices, seek remedial directions, adverse publicity orders and other punitive and non-punitive orders.

| Tier 1 contravention maximum penalty - the greater of: | Tier 2 contravention maximum penalty – the greater of: |
|--|--|
| 159,745 penalty units (which is currently \$50,000,185). | 31,950 penalty units (which is currently \$10,000,350). |
| Three times the total value of the benefit that the body corporate has obtained directly or indirectly and is reasonably attributable to the contravention. | Three times the total value of the benefit that the body corporate has obtained directly or indirectly and is reasonably attributable to the contravention. |
| If the court cannot determine the total value, 30% of the adjusted turnover over the body corporate during the breach turnover period for the contravention. | If the court cannot determine the total value, 10% of the adjusted turnover over the body corporate during the breach turnover period for the contravention. |

A regulator may seek multiple remedies for a single contravention. An important caveat is the civil penalty double jeopardy provision. If a person is ordered to pay a pecuniary penalty in respect of particular conduct, the person is not liable to pay another pecuniary penalty for contravention of another civil penalty provision of a principle or a sector-specific code in respect of that same conduct.

The Bill also creates a private right of action. A person who suffers loss or damage by the conduct of another person which contravenes a civil penalty provision of a principle or code may recover the amount of the loss or damage by action against that other person or against any other person involved in the contravention. This private right of action creates the risk of private class actions, especially if the loss or damage from a new and successful scam campaign is considerable.

What comes next

The Treasury consultation on the Bill was open for public consultation until 4 October this year. Feedback will assist to ensure the explanatory memoranda for the Bill aids the Parliament’s consideration of the proposed new law.

This short timeframe for consultation (three weeks) should support the government’s goal to introduce the final Bill to Parliament later this year. Despite the government’s ambition to establish the Scams Framework, the Bill will almost certainly be referred to Parliamentary committee for review.

Amid a busy legislative agenda, further delay risks the Bill not making it through this Parliament before the next Federal Election.

*For the full version of this article, please see: <https://www.gtlaw.com.au/knowledge/proposed-scams-framework-whole-ecosystem-approach-protecting-australians-scams>



THE CAMLA PODCAST



EPISODES 1 - 4 NOW STREAMING

Available at camla.org.au/member-downloads/

Important Cyber Security Reforms Tabled in Parliament and Referred to Committee

Authors: Sophie Dawson (Partner), **John Keeves** (Partner) and **Bianca Collazos** (Associate), Johnson Winter Slattery

The Australian Government has tabled its Cyber Security Legislative Package, which includes an obligation to notify the Department of Home Affairs and the Australian Signals Directorate (or another Department or statutory body specified in rules) within 72 hours of making or becoming aware of a ransomware payment in certain circumstances, and a framework for mandatory smart device security standards.

The Cyber Security Legislative Package was introduced into Parliament last Wednesday 9 October, and was referred to the Parliamentary Joint Committee on Intelligence and Security on 10 October. Submissions are due by 25 October 2024.

The Government has indicated that the package signals its commitment to address the growing global concern to strengthen cyber security and privacy protection. This follows the Government's introduction of the first tranche of long-anticipated privacy reforms into Parliament in September 2024, as covered in our article, '[Privacy law reforms unveiled in Canberra](#)'.

If passed, the Cyber Security Legislative Package will introduce standalone legislation to address cyber security, called the *Cyber Security Act 2024* (Cth) as well as amendments to the *Intelligence Services Act 2001* (Cth) and the *Security of Critical Infrastructure Act 2018* (Cth) (**SoCI Act**).

The reforms are aimed at addressing perceived gaps under the current legislative protections and in line with the Australian Government's vision to position Australia as a world leader in cyber security by 2030. The Bills would implement seven of the initiatives covered under the Government's *2023-2030 Australian Cyber Security Strategy* released in November 2023.

Proposed Cyber Security Act

The objects of the Cyber Security Act relate to enhancing the Government's capabilities to combat the threats posed by cyber security incidents and taking a 'whole of economy' approach to addressing the Government's cyber security concerns, including to:

- improve the cyber security of smart devices;
- encourage the provision of information to government about incidents, including in relation to ransomware payments;
- facilitate the whole of Government response to significant cyber security incidents through the National Cyber Security Coordinator; and
- prevent and improve the detection of and response to cyber security incidents through the establishment of the Cyber Incident Review Board.

Key measures

Key provisions included in the Cyber Security Bill are set out in further detail on page 35.

In addition to the Cyber Security Act, the Bills also progress reforms to the SoCI Act, including to clarify certain existing

obligations, simplify information sharing, introduce a new power for the Government to direct entities to address serious deficiencies in their risk management programs and bring aspects of regulation of the security of telecommunications into the SoCI Act.

Voluntary remediation and privacy reporting is commended OAIC closes investigation into 7-Eleven Stores

The Office of the Australian Information Commissioner (**OAIC**) has expressed its satisfaction with steps taken by 7-Eleven Stores Pty Ltd (**7-Eleven**) to voluntarily report its own conduct and undertake remediation of its privacy practices following a further privacy breach incident.

In 2021, the OAIC determined that 7-Eleven improperly used Facial Recognition Technology (**FRT**) during the collection of survey information from customers, in breach of its obligations under the Australian Privacy Principles. The OAIC concluded that during 2020, 7-Eleven had improperly collected sensitive information of customers without express or implied consent, using built-in cameras in tablet devices which captured images of customers as they filled out customer surveys instore.

The Australian Information Commissioner made a declaration that 7-Eleven must not repeat or continue this conduct. However, in 2023, 7-Eleven voluntarily notified the OAIC that the FRT system had been inadvertently re-enabled in some of its stores and improperly captured a further 45,874 facial images over a 12-month period before the feature was identified and promptly deactivated.

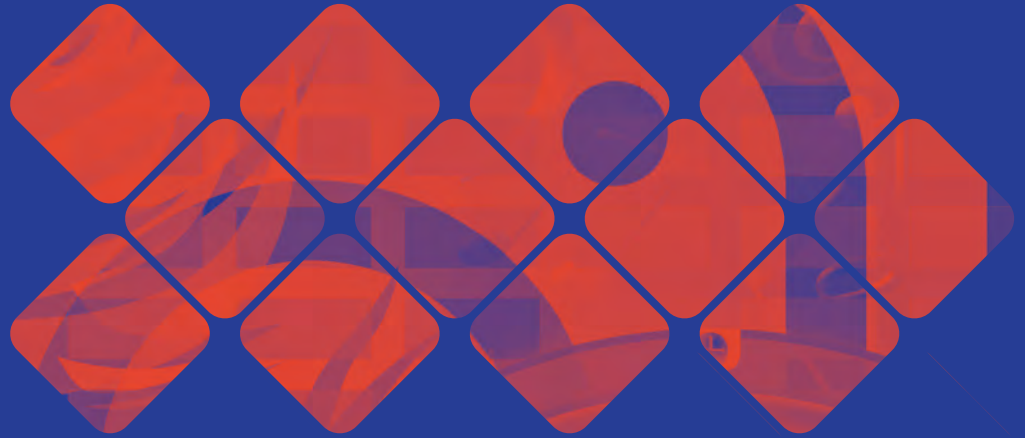
In September 2024, the OAIC closed its investigation, having been satisfied that 7-Eleven had "*adequately addressed the privacy deficiencies that led to the incident*" and that further action by the OAIC was not warranted. In closing its investigation, the OAIC considered several factors, including the inadvertent nature of the privacy incident, the prompt action taken by 7-Eleven to delete all facial images and the implementation of new measures to remedy the issue and prevent it from occurring in future.

Notably, the OAIC indicated its appreciation for 7-Eleven voluntarily reporting the incident, praising that it has '*acted consistently with the principles of good corporate governance and has assisted the OAIC in promoting and upholding the privacy rights of Australians*'. The OAIC commented that the use of FRT remains of concern and a regulatory priority and urged entities to ensure appropriate privacy measures are embedded from the outset, including before each new planned use of FRT and through implementing iterative testing of the robustness of privacy protections.

The OAIC's decision serves as a good reminder for businesses to remain vigilant and keep privacy obligations front of mind, particularly where sensitive information is captured such as through FRT systems. It is also important to take prompt action to address and remedy any privacy incidents. This determination illustrates the benefits of reporting incidents and working in cooperation with the OAIC as early as possible in appropriate circumstances.

Key provisions included in the Cyber Security Bill

| Measure | Overview | Effect of measure |
|---|---|--|
| Mandatory cybersecurity standards | <p>The Act would enable the Government to establish minimum cyber security standards for smart devices.</p> <p>These standards would be mandatory, and the Government indicated in the Second Reading Speech of the Bill that they are designed to bring Australia into line with international best practice and enhance consumer security, for example, to prohibit the use of universal default passwords on smart devices.</p> | <p>The rules may provide a mandatory security standard for relevant smart devices, being those which:</p> <ul style="list-style-type: none"> (i) are manufactured or supplied (other than second-hand goods) on or after the commencement of the Act; and (ii) otherwise meet the definition of 'relevant connectable product' including that the product can directly or indirectly connect to the internet that will be acquired in Australia in 'specified circumstances'. <p>This would require businesses who manufacture or supply the relevant products to:</p> <ul style="list-style-type: none"> (i) comply with the standards when they manufacture a product and are aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in those 'specified circumstances'; (ii) comply with any other obligations relating to the product; (iii) refrain from supplying non-compliant products where the supplier is aware, or could reasonably be expected to be aware, that the products will be acquired in Australia in those 'specified circumstances'; and (iv) provide and supply products in Australia with a statement of compliance with the security standard. <p>In relation to enforcement, the Act would provide powers for the Secretary of Home Affairs to:</p> <ul style="list-style-type: none"> (i) issue compliance, stop and recall notices for non-compliance; (ii) undertake an independent audit of a product; and (iii) request a statement of compliance and/or the product itself for the purposes of the audit at (ii) above. |
| Mandatory ransomware reporting | <p>The Government has proposed the introduction of mandatory ransomware reporting for certain businesses. These reporting obligations are intended to provide the Government with a better understanding of ransomware threats in Australia, with the goal of preventing further attacks and to assist businesses to recover following these types of incidents.</p> | <p>Under the proposed Act, certain entities who are impacted by a cyber security incident as defined (that has occurred, is occurring or is imminent), would be required to make a report to the relevant Department (ransomware payment report) where a ransomware payment has been made to an extorting entity.</p> <p>Relevant entities would be required to make the ransomware payment report within 72 hours of the making of the ransomware payment or becoming aware that the ransomware payment has been made.</p> <p>The entities subject to this obligation will be those who are (i) carrying on a business in Australia; and (ii) with an annual turnover in excess of the prescribed threshold in the Rules (proposed to be \$3 million to match the threshold in the <i>Privacy Act 1988</i> (Cth)); or (iii) entities who are a responsible entity for a critical infrastructure asset pursuant to Part 2B of the <i>SoCI Act</i>.</p> <p>A ransomware payment report must include particular information which is known or reasonably able to be found, including details relating to the impact of the cyber security incident, the demand made by the extorting entity and the ransomware payment which was made.</p> <p>If an entity fails to make a ransomware payment report they may be liable to a civil penalty (60 penalty units). However, an entity or its officers, employees or agents will not be liable where they have acted or omitted to act in good faith in compliance with their reporting obligation.</p> |
| Use and disclosure of reported information | <p>The Bill introduces obligations for the National Cyber Security Coordinator and the Australian Signals Directorate to limit the use and sharing of information which has been voluntarily provided by an entity affected by a cyber incident.</p> <p>The obligations are intended to operate together with other measures introduced through the Intelligence Services and Other Legislation Amendment (Cyber Security Bill) 2024 and are proposed to provide business with greater comfort to report cyber incidents.</p> | <p>In relation to information disclosed in a ransomware payment report or voluntarily provided to the National Cyber Security Coordinator, relevant government bodies would be obligated under the Act to:</p> <ul style="list-style-type: none"> (i) only use or disclose the relevant information for permitted purposes as specified. This includes for example, to assist the reporting entity and the Commonwealth or State body to respond, mitigate or resolve the cyber security incident; and (ii) not use or share the relevant information for specified purposes, including for example, regulatory action and for civil enforcement purposes for contraventions outside of the Act. <p>Civil penalties would apply to this section of the Act.</p> <p>The Bill also provides that the relevant information provided by the reporting entity would not be admissible in some proceedings, which includes most civil proceedings other than in relation to a contravention of the Act.</p> |
| Cyber Incident Review Board | <p>The Bill establishes the Cyber Incident Review Board (the Board), an independent advisory body intended to conduct reviews of cyber security incidents.</p> <p>In the Second Reading Speech of the Bill, the Government suggested it has modelled the Board from the United States Cyber Safety Review Board. The Board would have the ability to review the pre-incident circumstances, form its own findings and provide recommendations to the Government and to Industry.</p> | <p>The Board would be established and provided with the power to cause a review to be conducted in relation to certain cyber incidents.</p> <p>The reviews would be for cyber security incidents which:</p> <ul style="list-style-type: none"> (i) have or could reasonably be expected to seriously prejudice the social or economic stability, defence or national security of Australia; or (ii) involve novel or complex methods of technologies, where an understanding would significantly improve Australia's preparedness, resilience or response to similar cyber security incidents; or (iii) are or could reasonably be expected to be of serious concern to Australian people. <p>The review would be conducted by a review panel and the purpose of these reviews would be to make recommendations to government and industry regarding measures which could be taken to prevent, detect, respond to or minimise the impact of similar cyber security incidents in future.</p> <p>Under this measure, the Board would be provided with the power to request and compel the production of information and documents relevant to the review from particular entities. Civil penalties would apply to a failure to comply with a notice to produce document under the relevant section.</p> <p>Similar provisions (as set out above) regarding the use, disclosure and admissibility of the information would also apply to information relating to reviews</p> |
| Voluntary information sharing with the National Cyber Security Coordinator | <p>The Bill provides entities with the option to report significant and potentially significant cyber security incidents to the National Cyber Security Coordinator. This is to enable the National Cyber Security Coordinator to lead the response across the whole of Government.</p> | <p>The Bill contains limits on the use and disclosure by the National Cyber Security Coordinator of information provided in voluntary reports to encourage voluntary reporting.</p> |



About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants.

Issues of interest to CAMLA members include:

- Defamation • Contempt • Broadcasting • Privacy • Copyright • Censorship • Advertising
- Film Law • Information Technology • Telecommunications • Freedom of Information
- The Internet & Online Services

In order to debate and discuss these issues CAMLA organises a range of seminars featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For Further Information:

Visit the CAMLA website at: www.camla.org.au for information about CAMLA, CAMLA seminars and events, CAMLA membership options and fees, competitions and the Communications Law Bulletin.

