Safe and responsible AI in Australia: Discussion paper

Submission from elevenM

9 August 2023

Contents

Introduction

Over the last two decades, digital innovation has resulted in a wholesale transformation of economies around the world. Over the next two decades AI and related technologies promise even more radical change, with the potential to disrupt virtually every aspect of our economy and society. In this nascent space, the opportunity for Australia is immense. We are well placed to shape the global debate on responsible AI policy, and Australian businesses are already taking a leading role in responsible AI development. The challenge for government is to put in place regulatory settings that will drive responsible innovation while capturing the benefits for all Australians.

At elevenM, we believe that trust is a critical dependency for sustained digital innovation, and the establishment and maintenance of trust should be a guiding star for technology policy. Trust unlocks business' license to innovate and enables public participation in the benefits of new technologies. Without trust, adoption falters and progress stalls.

AI regulation should be focused on building trust in AI systems by managing risk and ensuring AI development and use is well aligned to community values and expectations.

Regulation should apply to public and private organisations and address all sources of risk across the AI supply chain, including developers and deployers of solutions. It needs to allow flexibility in some areas (which can be achieved with a risk-based model) and be more stringent in others (such as banning activities with the potential to cause real harm to people). Our regulatory regime must be consistent with emerging international standards, and it must be overseen and maintained by a well-resourced and active regulator. In short, this regime must have teeth. Neither self-regulation nor limited focus on certain AI supply chain participants will deliver the consistency and reliability of outcome required to build public trust and drive adoption of new AI technologies.

About elevenM

elevenM is a specialist privacy and cyber security consultancy. Our mission is to build trust in an online world.

Our team comprises experts in complementary disciplines such as AI, privacy compliance, operations and technology, strategy, public policy, risk and compliance, IT risk, supplier risk, data governance and cyber security.

Members of our team combine technical and legal qualifications with extensive experience in the field. We work hand in hand with our clients to understand their businesses and identify effective and efficient solutions which are suitable for them — not only for today but for the constant changes coming over the horizon.

We work closely with organisations in the public and private sector to implement AI ethics, privacy and security programs, including improving transparency, delivering training and awareness initiatives, managing risks, remediating after breaches, conducting impact assessments, assessing vendors and third-party supplier frameworks, embedding ethics, privacy and security by design and more.

Submission

Definitions

Question 1: Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?

elevenM position	Definitions should be drafted with the following goals: • global interoperability and alignment with definitions adopted in key economic markets; and • durability in a rapidly changing technological environment. Key participants across the AI supply chain should also be defined and within the scope of any regulatory response to AI, including providers of inputs, developers, providers and users of AI systems.

Durability and global interoperability

The definition of 'artificial intelligence' used in the Discussion Paper is based on the definition adopted by ISO/IEC 22989:2022(en) but differs from the ISO definition by requiring that AI systems generate 'predictive' outputs 'without explicit programming'. It is not clear whether the proposed definition was so drafted with the intent of being narrower than the ISO/IEC definition, for example by excluding logic or knowledge-based approaches, such as symbolic reasoning and expert systems.

The definition offered in the Discussion Paper also differs from definitions adopted by the OECD and by the European Union (which are similar to each other but not identical).

In our view, the proposed definition of AI would likely be narrower than any of the ISO/IEC, OECD or EU definitions, and in particular may exclude some logic and knowledge-based systems that would be covered by those definitions. We submit that this would be a bad outcome, both for reasons of consistency and because such systems can pose many of the same risks.

In general, in the interests of global interoperability, Australia should seek to align definitions of key terms with emerging international standards and definitions adopted by key trading partners. Any departure from established definitions for the Australian context is likely to lead to increased cost and complexity for Australian businesses, whether they are looking to compete in global markets or import AI systems for domestic use.

Definitions should aim to be technology neutral and focus on substance over form to ensure durability in a rapidly changing technological environment. Where reference to particular techniques or technologies are required, these should be made in the most general terms possible. Both the EU AI Act and the ISO Standard include supplementary notes to the definition of AI which emphasise that the definition is intended to cover a range of techniques

and approaches.[1] We recommend that any Australian legislative definition of 'artificial intelligence' be similarly supported by a non-exhaustive list of covered techniques and approaches. Such a list could be included in regulation so as to be more easily kept up to date.

Defining participants across the entire AI value/supply chain

In order to achieve safe and responsible AI, the scope for AI regulation must be broader than just models and their application. It is important that regulators define and consider risks to and arising from participants throughout the AI supply chain, including:

- raw data used to build and train models (and the means by which that data is gathered and aggregated);
- compute power, including supply chains and environmental costs of both manufacturing hardware and running massive data centres required for AI products;
- manual labour involved in coding and labelling large datasets, or moderating outputs;
- creation of foundation models on which AI applications can be built;
- specific purpose applications that deploy a particular model or approach for a specific use case;
- services surrounding the deployment or optimisation of AI applications; and
- direct and indirect impacts of AI applications.

Potential gaps in approaches

Question 2. What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?

elevenM position	Risks associated with the use of facial recognition are not covered by Australia's existing regulatory approaches but could be addressed through a risk-based framework such as that proposed by the University of Technology Sydney's Human Technology Institute's Facial recognition model law. More generally, regulatory intervention is required to: • provide nationally consistent protections; • protect against discriminatory, arbitrary or unfair algorithmic decisions that aren't made on the basis of a protected attribute; • guard against cumulative and systemic risks; and

[1] See ISO/IEC 22989:2022, section 3.1.4 <https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:22989:ed-1:v1:en:term:3.2.10> and Recital 6 of the current text of the European Artificial Intelligence Act, see: *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html>.*

- provide effective recourse where algorithms cause diffuse harms (i.e., minor-moderate harm across a large group of people).

Finally, some risks arising from the AI supply chain (carbon emissions from training, extractive materials and exploitative labour practices) are inherently global, requiring management through global governance initiatives.

Facial recognition, law enforcement and the Privacy Act

Currently, the main way facial recognition technology is regulated is through the *Privacy Act 1988* (Privacy Act). The OAIC investigations into Clearview AI and AFP's practices demonstrates some of the challenges of effectively protecting Australians' rights despite investigation findings of breaches to the Privacy Act.

As noted in the Discussion paper, the OAIC found Clearview AI had breached the Privacy Act by covertly scraping biometric information online without consent.[2] On finding breaches to the Privacy Act, the Privacy Commissioner ordered Clearview AI to cease collection of facial images and biometric templates and to destroy existing images and templates collected from Australia.

The OAIC further determined that the AFP failed to conduct appropriate privacy assessments, observing a lack of governance, risk and assessment or controls within the AFP in their use of facial recognition technology developed by Clearview AI.[3] Importantly, the AFP's actual use of Clearview AI did not breach the Act – only their failure to conduct a privacy assessment before deploying the tool. This is because the Privacy Act provides broad exceptions for the collection, use and disclosure of personal information (including in biometrics, AI or automated decision-making) for law enforcement purposes, so virtually any actual use of facial recognition is permitted – provided the agency goes through the motions of a privacy impact assessment first.

The press has reported that the AFP and Clearview continue to explore together the deployment of facial recognition technologies for Australian law enforcement purposes.[4] And under the OAIC's determination, they are permitted to do this.

The Clearview AI case demonstrates that aside from a requirement to complete a PIA, the Privacy Act ultimately sets no concrete guardrails in relation to law enforcement's use of facial recognition. This is despite significant risks to human rights should it be misused, overused or used in error in that context. We strongly recommend that in addition to a mandatory PIA, a stringent regulatory regime be introduced governing use of facial

[2] 'Safe and responsible AI in Australia' (Discussion paper, Department of Industry, Science and Resources, 2023), available at https://consult.industry.gov.au/supporting-responsible-ai.
[3] Office of the Australian Information Commissioner (OAIC), 'AFP ordered to strengthen privacy governance' (Media Release, 16 December 2021), available at https://www.oaic.gov.au/newsroom/afp-ordered-to-strengthen-privacy-governance.
[4] Cam Wilson, 'AFP secretly met with Clearview AI months after being told to not use it, emails reveal' Crikey (online) 5 July 2023, available at https://www.crikey.com.au/2023/07/05/clearview-ai-australian-federal-police-facial-recognition.

recognition technology in law enforcement, in line with that proposed by the UTS Human Technology Institute.[5]

Facial recognition in the private sector

Recent reports from CHOICE have shown that facial recognition is being deployed at scale within the private sector as well, often with minimal transparency and few controls.[6] Alarmingly, in some cases facial recognition technologies are being deployed in semi-public spaces by companies that also have significant businesses in the sale and aggregation of data about people.[7] Facial recognition is being deployed either on the basis that consumers consent (a proposition that is difficult to sustain given most consumers are unaware of its use)[8] or that it is reasonably necessary for preventing a serious threat to life, health or safety, or to take appropriate action in relation to suspected unlawful activity or serious misconduct. As with the exceptions for law enforcement discussed above, these exceptions provide broad permissions for organisations to use potentially risky AI technologies with minimal oversight.

Proposals in the Attorney-General's Department's Privacy Act Review Final Report[9] may go some way to addressing these issues, but would not address broad exceptions relating to law enforcement and unlawful activity that permit deployment of high-risk AI technologies with minimal oversight.

Systemic risks

Additionally, privacy law is poorly placed to identify and manage systemic risks. In the case of facial recognition, there is a cumulative risk to privacy and civil liberties that grows with widespread deployment of facial recognition across many different venues. If retailers and public spaces all have facial recognition enabled cameras in place, the effect will be that people are identified everywhere they go, and the same systemically vulnerable cohorts –

---

[5] Nicholas Davis, Lauren Perry and Edward Santow, 'Facial Recognition Technology: Towards a Model Law' (Report, Human Technology Institute, The University of Technology Sydney, 2022) 72-74, available at https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf ('*HTI FRT Model law*').

[6] Jarni Blakkarly, 'Kmart, Bunnings and The Good Guys using facial recognition in stores', *CHOICE* (online), 12 July 2022, available at https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store.

[7] Jarni Blakkarly, 'Facial recognition in use at major Australian stadiums', *CHOICE* (online) 5 July 2023, available at https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/facial-recognition-in-stadiums.

[8] CHOICE canvassed 1000 Australians between March and April 2022 and found that more than three in four respondents (76%) said they were unaware retailers were using facial recognition: Blakkarly, above n 6.

[9] 'Privacy Act Review' (Report, Attorney General's Department, 2022), available at https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf. See, for example, proposal 11 to amend and strengthen the definition of 'consent'; proposal 12 for a requirement that personal information handling be 'fair and reasonable'; and proposal 13.1 for a mandatory Privacy Impact Assessment for high risk activities in the private sector.

people of colour, women, children, people with disabilities[10] – will be disproportionately affected by failures. While no individual deployment may be in breach of the Privacy Act, the cumulative surveillance and discrimination is nevertheless inconsistent with our liberal democratic values.

National consistency and the limits of anti-discrimination law

Key areas of harm are under the jurisdiction of the states and territories. We will need uniform law initiatives akin to the Commonwealth-State initiative for uniform defamation laws. A notable example is the use of AI by the real estate industry in residential tenancy applications which undermines human rights of renters – one-third or more of the adult population.

Academic research in Australia and elsewhere has shown how new technologies including AI can accelerate existing social, economic and political inequalities and discrimination,[11] and State and Territory Residential Tenancies Acts are silent on such matters, creating opportunities for discriminatory and unethical uses of data without consequences by agents. As the risk and nature of the harm is so significant, direct regulation may be justified. Transparency is of little use when the power imbalance between the target of the automated decision-making and the decision-maker is so stark.

Notably the nature of this type of discrimination (on the basis, for example, of some past late rental payment) does not fall foul of anti-discrimination laws as a person who had past financial difficulties is not a protected attribute.

Amplification of risks and harms for children

Several risks which are covered in this paper are exacerbated for children and vulnerable people, hence, capacity to protect children and vulnerable people must be the litmus test for proposed frameworks and guardrails. Take for example, the constraints of transparency, literacy and consent. Given that the concepts and potential harms and benefits of AI are poorly understood by adults, minors (and certain vulnerable people) cannot reasonably bear the onus of assessing risks and giving valid consent to AI-led processes. Also, adverse impacts such as false attribution of characteristics leading to discrimination (for example in the context of facial recognition for law enforcement or automated decision-making regarding access to social welfare or services) can endure for a young person well into adulthood. We submit that the standard of protection offered Australia's future AI governance framework must be tested against its ability to protect the most vulnerable people in our society, including children.

Addressing diffuse harms

By its nature, AI permits action at scale. In the privacy context, academics have observed how high legal thresholds for recognisable harm can lead to minor harms being ignored, and

---

[10] See *HTI FRT Model law*, above n 5, page 28.
[11] See, eg, Sophia Maalsen et al, 'Understanding discrimination effects in private rental housing' (Final Report No. 363, Australian Housing and Urban Research Institute, 2021), 15-16, available at https://www.ahuri.edu.au/research/final-reports/363.

may even lead to acclimatisation to more significant intrusions.[12] Where AI and automation is deployed at scale, a similar risk arises: that small, frequent and mundane harms from AI systems fall below the threshold for legally compensable harm in any individual case, and so must be tolerated. Any regulatory regime should include mechanisms for addressing these kinds of diffuse harms, for example by provision for class actions or through a central regulator or ombudsman - with sufficient resources to meet forecasted need into the future.

Global harms

As we have argued in response to question one, the scope for AI regulation must be broader than just models and their application. The AI supply chain presents significant risks that extend beyond Australia's national borders, and which will require transnational governance initiatives to manage:

- Environmental risks from model training.
    - Model training requires immense amounts of computation, which in turn requires significant resources – power to train models, water for cooling data centres, and rare minerals for constructing computer hardware; and
- Labour and human rights risks from data labelling.
    - Today's AI systems rely on large amounts of human labour, to label data and to moderate or fine-tune outputs.[13] At present, this labour is often sourced from the global south, with limited assurance of safe or equitable working conditions.

While environmental risks and labour conditions outside of Australia may not be within scope for direct regulation in an Australian 'AI Act', these issues should be considered in Australia's broader regulatory response. Australia has been credited as a global leader in combatting modern slavery in the supply chains of products that we use every day, including electronics, garments, solar panels and textiles.[14] We should aspire to a similar leadership role in driving standards for the ethical production of AI systems, as similar risks are already arising around data labelling and content moderation.

[12] Woodrow Hartzog, Evan Selinger and Johanna Gunawan, 'Privacy Nicks: How the Law Normalizes Surveillance' (2023) 101 *Washington University Law Review*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384541.
[13] Josh Dzieza, 'AI is a lot of work', *The Verge* (Online), 20 June 2023, available at https://www.theverge.com/features/23764584/ai-artificial-intelligence-data-notation-labor-scale-surge-remotasks-openai-chatbots.
[14] Walk Free 2023, 'The Global Slavery Index 2023' (Minderoo Foundation, 2023), available at https://walkfree.org/global-slavery-index.

Question 3. Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.

elevenM position	Domestic and global networks should be harnessed for greater uniformity and consistency allowing organisations to easily meet national and global compliance requirements. Government procurement standards also present a powerful non-regulatory policy lever to drive safe and responsible AI standards.

Australia is well placed to lead international approaches

Australia is well placed to play a leading role to shape international approaches to the regulation of AI and must position itself within global initiatives.

By way of analogy, in the privacy space, the OAIC has successfully coordinated joint investigations with international counterparts, including:

- A joint investigation with the UK Information Commissioner into Clearview AI's personal information handling practices;[15]
- A joint investigation with the Privacy Commissioner of Canada in Ashley Madison's personal information handling practices; and[16]
- A joint Australia-New Zealand investigation into Latitude group's personal information handling practices.[17]

The OAIC has a Memorandum of Understanding (MOU) with the UK ICO[18] and the Data Commissioner of Ireland[19] to strengthen enforcement and provide mutual assistance.

[15] OAIC, 'OAIC and ICO conclude joint investigation into Clearview AI' (Media Release, 3 November 2021), available at https://www.oaic.gov.au/newsroom/oaic-and-ico-conclude-joint-investigation-into-clearview-ai.
[16] 'Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner' (Office of the Privacy Commissioner of Canada and OAIC, 2016) available at https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/investigation-reports/ashley-madison-joint-investigation.
[17] OAIC, 'Joint Australia–New Zealand investigation into Latitude group' (Media Release, 10 May 2023), available at https://www.oaic.gov.au/newsroom/joint-australianew-zealand-investigation-into-latitude-group.
[18] OAIC, 'OAIC and the UK's ICO sign memorandum of understanding' (Media Release, 20 March 2020), available at https://www.oaic.gov.au/newsroom/oaic-and-the-uks-ico-sign-memorandum-of-understanding.
[19] 'MOU with the Data Protection Commissioner of Ireland' (MOU, OAIC), available at https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/mou-with-the-data-protection-commissioner-of-ireland.

The OAIC and Privacy Commissioner has also played a significant and often a leading role in the Asia-Pacific Privacy Authorities (APPA) Forum[20] having previously provided Secretariat role, and synchronised global Privacy Awareness Week campaigns.[21]

Such forums facilitate opportunities to develop a consistent global approach to AI regulation, provide a forum to open and/or closed discussions to share regulatory enforcement experiences, challenges and enhanced international regulatory cooperation. The APPA forum is an example of the strength and benefits of a united and global cooperation in the regulation of privacy and data security.

Australia in a strong position and has an opportunity to lead discussions to ensure alignment and interoperability of any AI regulatory framework, as we have in privacy. Further, if Australia does not position itself to work collaboratively in AI regulation, there is a risk of exclusion from international frameworks and initiatives.

Government is well placed to lead domestically

The Australian Government is well placed to model best practice by adopting a high standard of AI governance internally and committing to public shing frameworks, guidance and case studies around successful and unsuccessful AI deployments (see question 7 below).

Government procurement standards

Government procurement standards also present a powerful non-regulatory policy lever to drive safe and responsible AI standards. Government is a major buyer of information and communications technologies and can use its significant market power to drive higher standards from suppliers or establish expectations of suppliers that other purchasers can then leverage. This can be effective in a range of domains, from raising environmental or labour standards to improving cyber security.[22]

A first step could be to drive transparency by requiring all suppliers of AI to government to provide model cards[23] (or meet a similar transparency standard). Model documentation and transparency present an ideal use case for influence by procurement standards because once produced for government, transparency documentation can be made available for other users at minimal marginal cost.

---

[20] Asia Pacific Privacy Authorities (APPA), *Home,* available at https://www.appaforum.org/.
[21] OAIC, 'Privacy: 'Back to Basics' – Joint statement by Privacy Authorities Australia' (Media Release, 1 May 2023), available at https://www.oaic.gov.au/newsroom/privacy-back-to-basics-joint-statement-by-privacy-authorities-australia.
[22] Rajiv Shah, 'Cybersecurity must be a key part of Australian government procurement decisions' *The Strategist* (online) 18 August 2020, available at https://www.aspistrategist.org.au/cybersecurity-must-be-a-key-part-of-australian-government-procurement-decisions/.
[23] Margaret Mitchell et al, 'Model Cards for Model Reporting' (Paper presented at FAT* '19: Conference on Fairness, Accountability, and Transparency, Atlanta, USA, 29–31 January 2019), available at https://arxiv.org/pdf/1810.03993.pdf.

Question 4. Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.

elevenM position	AI governance requires coordination across policy and regulatory domains, and across jurisdictions. Coordination should focus on building and sharing capacity across the public sector and driving consistency in AI regulation. From individuals' perspective, coordination should support trust by streamlining access to remedies when things go wrong.

AI harms will not fall neatly within one policy or regulatory domain. We support the continuance of forums such as DP-REG to combat the divergence of technology governance and regulation across government today. AI governance should utilise these cross-portfolio approaches to facilitate collaboration and the development of literacy and awareness within each specialised regulatory body.

AI harms will also not fall neatly within a single Australian jurisdiction, and with key areas of harm under the jurisdiction of the States and Territories, cross-jurisdictional collaboration will be critical. Privacy Authorities Australia is an example of an effective forum for cross-jurisdictional coordination within Australia. Such forums allow Commonwealth, state and territory privacy regulators to provide updates on significant developments within their jurisdiction and a platform to share knowledge and resources in tackling emerging issues. This helps encourage consistency and uniformity in AI regulation, leading to more certainty for businesses when it comes to compliance with various regulatory frameworks.

For individuals adversely affected by AI, the appropriate complaint pathway may be difficult to identify. Australian regulators should collaborate to maintain a 'single front door' or 'no wrong door' approach for complaints, ensuring that all concerns are directed to the correct regulatory domain to ensure that they are managed appropriately. Access to effective recourse when things go wrong will support greater public trust in AI.

Responses suitable for Australia

Question 5. Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

elevenM position	In addition to aiming for interoperability and consistency across jurisdictions, Australia should remain focused on protecting our established liberal democratic values (including human rights).

The European approach to regulation through the AI Act presents many features that are adaptable and desirable for Australia. In particular, the AI Act demonstrates a focus on protecting established liberal democratic values (including human rights) and aims to only apply substantial compliance obligations where there are significant risks.

In addition, transparency requirements for foundation models proposed in the EU (which include disclosure of copyrighted data used in model training) are likely to enable rights-holders to better police their existing rights against misuse by AI developers. This is an effective model that can be applied to AI regulation at large. That is, one of the key roles for AI regulation should be ensure that new technologies and practices associated with the development or deployment of AI remain subject to existing laws.

Target areas

Question 6. Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?

elevenM position	AI regulation should build trust by managing risk. We don't believe that the regulatory approach should be materially different between public and private sector uses.

AI regulation should be focused on building trust in AI systems by managing risk and ensuring AI development and use is well aligned to community values and expectations. With this in mind, we don't believe that the regulatory approach should be materially different between public and private sector uses.

However in practice, we expect to see government generally adopting higher standards of governance over AI than the private sector for several reasons, including to model best practice or to live up to general obligations to the public interest. Additionally, government use of AI will more often be higher risk than private sector use, due to the types of services governments provide, the likelihood that government services will affect individuals' rights, and the absence of market choice for individuals using government services (or subject to government power).

Question 7. How can the Australian Government further support responsible AI practices in its own agencies?

elevenM position	The Australian Government should invest in best practice AI governance within its own agencies.

In the cyber security context, the Australian Government acts as an exemplar for industry by designing and implementing best practice, providing transparent assurance and reporting, and developing policies and guidance for broader use. This approach recognises the fact that as a nation, we are only as strong as the weakest link and therefore all participants must guard against cyber vulnerabilities. This approach also allows government to build public trust by maintaining its own high standards, while developing human capital and practical guidance that can be leveraged by industry.

An equivalent approach is necessary within the AI space, to protect the human rights of individual citizens and society. To this end, the Australian Government could:

- Prioritise Australian Government agencies as being the benchmark for safe and responsible AI practices, including but not limited to:

    - adopting harm reduction frameworks and policies;
    - maintaining clear frameworks and guidelines in the pursuit of best practices; and
    - submitting to external review / auditing as appropriate.
- Commit to publishing frameworks, guidance and case studies around successful and unsuccessful AI deployments.
- Commit to training and developing of government staff / talent in safe & responsible AI practices.
- Leverage its market power to drive transparency and other outcomes from AI suppliers (see question 3 above).

Question 8. In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.

elevenM position	Wherever possible, generic or established legal and governance frameworks should be relied on to manage AI risk. Technology-specific solutions or requirements should seek to bridge the gap between novel technologies and existing risk management mechanisms. Technology-specific solutions or requirements may also be appropriate to allocate responsibility efficiently or to clarify individuals' rights.

Our expectations for the outcomes of AI regulation are well established by Australian and liberal democratic values, and are embodied in Australia's AI Ethics Principles, as set out on page 14 of the Discussion paper. In most cases, existing, technologically neutral laws and governance mechanisms are well adapted to achieving these outcomes whether AI is involved or not — employers are responsible for the health and safety of their employees at work, companies have well established frameworks for managing and reporting on risks of all types, producers are responsible for the safety and reliability of their products, and so on.

Technology-specific requirements should not duplicate existing laws or risk-management frameworks, but should instead seek to bridge the gap between novel technologies and existing concepts and processes.

For example, cases arise where existing laws covering potential harms (copyright, discrimination, consumer protection, privacy, etc) are of limited effectiveness because wronged parties aren't aware that an AI system was in play or aren't able to access relevant details about the system and how it works.

Similarly, generic corporate procurement and risk management processes may be well adapted to manage risk generally, but may be ineffective at managing AI risk due to a lack of access to relevant data about the operation or performance of a system or because of a company's inability to influence a large vendor.

In both cases, there is a need for regulatory intervention requiring transparency and explainability (potentially including overriding claims of trade secrets or commercial-in-confidence) in order to make AI systems amenable to existing laws and frameworks.

Technology specific requirements can allocate responsibility more efficiently

Generic requirements are an appropriate means by which all organisations that deploy AI can be required to work through a process or framework to ensure the deployments formally identify and minimise risks. These activities can be guided by well-established risk management frameworks.

Simultaneously there is value in technology specific regulations that place obligations on the developers of AI, to guide how they design and build solutions and remediate identified risks. This two-pronged approach has parallels in cyber security public policy, where for a long time there have been regulations and expectations that place obligations on the deployers of information technology, i.e., organisations. However we are now seeing a focus on the need to place greater responsibility for safety and security on the vendors and manufacturers of technology products, who are best placed to secure those products.

Access to justice is served by clearly defined requirements

Specific requirements give people confidence to pursue their rights. If legal claims have to be shoehorned into generic protections, they will be more risky and less likely to be pursued. For example, an individual subject of defamatory statements produced by an AI system will be much less likely to pursue their rights if to do so would require expensive litigation to establish whether a large language model is a 'publisher'.[24]

Question 9. Given the importance of transparency across the AI lifecycle, please share your thoughts on:

a. **where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?**

b. **mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.**

elevenM position	Transparency is critical but should not shift the onus of risk management to the individual.

Transparency is necessary but not sufficient for public trust

Meaningful and effective transparency for end users of AI systems will be necessary to maintain public trust. Transparency obligations should include disclosing when a user is interacting with an automated system, when content is automatically generated (e.g., via watermarks) and when and how automated systems are being used to make decisions affecting a person's rights or interests.

[24] See, eg: Simon Newcomb and Ian Bloemendal, *It's not a lie, says generative AI: untruths, defamation and the use of ChatGPT* (3 May 2023) Clayton Utz, available at https://www.claytonutz.com/knowledge/2023/may/its-not-a-lie-says-generative-ai-untruths-defamation-and-the-use-of-chatgpt.

However, there is a growing consensus among privacy experts, civil society organisations and legislators that the historic focus of privacy regulation on transparency and consumer choice has failed, and that new laws are required to shift accountability for privacy protection to organisations using our data.[25]

Transparency rarely benefits consumers directly. Transparency requirements have been central to privacy law since the 1980s, yet today only 21% of Australians report always or often reading privacy policies, and only 32% feel in control of their privacy.[26] This is unsurprising, as most privacy policies make it difficult for individuals to understand how their personal information and data is being used, and few have the time or inclination to read 2500 words for every website we visit or service we use.[27]

Transparency does, however, play a key role in privacy regulation by providing consumer advocacy groups and regulators with access to key information, and by putting companies on the record about what their products do. We suggest that the role of transparency in AI regulation is best thought of in similar terms.

Deployers and regulators require information to manage risk

The risks and impacts of AI systems can only be managed with access to information about those AI systems across their supply chain or lifecycle.

Information about the inputs (data, labour, resources) to a system is required to understand its environmental and social costs, as well as whether it contains any inherent biases, or whether it complies with privacy, intellectual property and copyright regulations.

Therefore, access to information about data processing algorithms is required to assess the accuracy and reliability of outputs. In particular, procurers require access to meaningful and standardised metrics about the performance of AI systems in order to make accurate risk assessments prior to deployment.

---

[25] See, for example, elevenM, *Privacy in focus: The consent catch-22* (23 March 2021), available at https://elevenm.com.au/blog/privacy-in-focus-the-consent-catch-22; Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy (23 March 2020) New America, available at https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/.*

[26] OAIC, *Australian Community Attitudes to Privacy Survey 2023* (2023) 18-19 and 21, available at https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf.

[27] See, for example, Alexis C. Madrigal 'Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days', *The Atlantic* (online) 1 March 2012, available at https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

10. Do you have suggestions for:

a. **Whether any high-risk AI applications or technologies should be banned completely?**

b. **Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?**

elevenM position	We support targeted bans on applications or technologies that present unacceptable risks to human rights or public interests. We support a moratorium on certain high-risk uses of facial recognition and biometric technology pending the introduction of governing legislation.

Bans have the benefit of sending a clear and simple message about the bounds of acceptable behaviour. Clear messages can help engender trust and may encourage more people to use AI with confidence that the most concerning applications will under no circumstances be permitted.

Bans are appropriate where applications or technologies present unacceptable risks to human rights or public interests without any countervailing benefits. Criteria or requirements for identifying applications or technologies to be banned should be no different to the criteria on which applications or technologies are risk-rated. For example, the Canadian *Personal Information Protection and Electronic Documents Act* presents an example of qualitative criteria (that covered organisations must only handle personal information for purposes that a reasonable person would consider appropriate in the circumstances) that amounts in effect to a categorical prohibition on certain types of behaviour.[28]

Bans should be applied as narrowly and specifically as possible, and may be timebound or subject to regular reviews. The risks associated with any AI application or technology will always be highly dependent on context, and any prohibition on a class of applications or technologies risks capturing beneficial uses as well.

We support limited moratoria on specified applications of certain high-risk technologies on a case-by-case basis. For example, we support the recommendations of the Human Rights Commission for a moratorium on the use of facial recognition or other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement, pending the introduction of legislation that protects human rights.[29]

[28] Guidance from the Office of the Privacy Commissioner of Canada calls these prohibited practices 'no-go zones', and they include handling of personal information that is otherwise unlawful, or profiling and categorisation that may lead to unfair, unethical or discriminatory treatment contrary to human rights law: Officer of Privacy Commissioner Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (May 2018), available at https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.

[29] See recommendations 19 and 20 of the Australian Human Commission, 'Human Rights and Technology' (Final Report, 2021), available at https://humanrights.gov.au/our-work/technology-and-human-rights/publications/final-report-human-rights-and-technology.

11. What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

elevenM position	Clear and effective regulation will drive innovation by giving industry certainty and adoption by building public trust. Open dialogue about the true risks of AI, and how these are being managed, will also enhance public literacy around AI and AI safety, and support increased confidence and adoption over time.

Regulation and oversight of AI technology that protects people from harm is the best and only way to drive public trust. Systems must be safe and effective and be seen to be so. Individuals and businesses, if harmed, must have access to remedies. Trust must be earned, but with trust comes social license to innovate, and confidence to adopt. Clear and effective regulation also provides greater certainty for industry to innovate with AI in a safe way.

We observe a significant increase in public dialogue around AI and AI safety in recent months, with contributions from governments, businesses, media and civil society. However, the conversation has in our view, been unhelpful at times, by either minimising the risks of AI or focusing excessively on extreme and unfounded risks such as imminent existential threats from sentient AI.

We believe trusted institutions – including the government, academia and businesses – have an important role to play in shaping a more constructive conversation around AI. A collective discourse that highlights real risks and opportunities of AI and builds understanding about how these are being mitigated or pursued. Such a conversation will create a foundation for a more AI-literate community, and support more confident use of this technology. There is a role for the Australian government in particular to build Australians' confidence in AI by establishing guardrails and showing leadership within the global dialogue.

Implications and infrastructure

12. How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?

elevenM position	We expect banning certain very high-risk activities or technologies is most likely to provide a net benefit to Australian tech trade and exports through alignment with regulation in key markets such as the EU.

Bans on a small number of very high-risk activities or technologies (like social scoring or facial recognition technology in certain circumstances) are likely to be necessary to ensure alignment with international human rights standards, as well as interoperability with key technology trading partners such has the EU. We see such alignment and interoperability as more likely to provide a net benefit to trade and export for Australia's tech sector by minimising compliance costs when engaging with a major market. We have seen this play out in the privacy context, where countries such as Israel have deliberately aligned with the EU's GDPR to provide significant benefits for tech trade and exports.

13. What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks? Risk-based approaches

elevenM position	No comment.

14. Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?

elevenM position	We support a risk-based approach to regulating applications of AI but note that additional regulation will be required to address risks arising from other parts of the AI supply chain, such as inputs (e.g., data, labour, resources) and model development.

We support a risk-based approach to the regulation of AI applications. Risks and harms of AI technology vary with application, and compliance obligations should be commensurate.

The risk-based approach works best when applied to 'deployers' of AI technology in relation to a specific, well-defined product or use case. For example, where a financial services organisation uses an AI-based scoring algorithms to make a credit assessment.

However, we also recommend that additional specific consideration be given to participants of the AI supply chain and ecosystem where a focus on application or deployment does not fully cover the range of risks, such as:

- More general or 'foundation' models (such as foundation models for large language models such as ChatGPT, Bard, and others) or even specifically trained models that might be deployed in a variety of contexts for a variety of purposes (e.g., Facial recognition) – see question 19.
- 'Development' of models, including issues arising from training data used, labour used to code data or moderate outputs, system design choices, security, carbon emissions, assurance and transparency about performance.

Additionally, as discussed at question 9 above, risk management by the deployers of AI systems will require model developers to provide meaningful transparency around model inputs and performance. Regulation should seek to secure a degree of business-to-business transparency to enable effective risk assessment and management.

15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?

elevenM position	A risk-based risks leaving too much in the hands of industry self-assessment, and may overlook systemic or second order risks.

A risk-based approach will require monitoring and enforcement from a well-resourced regulator in order to ensure consistent assessment of risks across industries and technology types. Without clear guidelines and strong enforcement, a risk-based approach (where the

legal requirements depend on a self-assessment by an organisation) can be at best uncertain and at worst gamed or co-opted.

Risk-based approaches can be overly focused on single deployments or use cases and may not address systemic or second order risks arising from widespread adoption of technologies or interactions between technologies. A central supervisory authority will be important to provide a whole-of-system view and respond to risks that may arise from cumulative adoption of a technology across the economy.

16. Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?

elevenM position	Risk-management is well understood and will not require companies to 're-invent the wheel' by creating new, AI-focused compliance structures. However, a risk-based approach risks leaving too much in the hands of industry self-assessment, and may overlook systemic or second order risks.

The risk-based approach may need to be adapted to accommodate smaller organisations that will not have the resources or expertise to effectively conduct risk assessments, but will nevertheless be attracted to AI technologies. Risk management requirements can be framed to be commensurate with the size and scale of businesses in the same way as 'reasonable steps' requirements in the Privacy Act allow organisations to take their own available resources into account when evaluating the cost-benefit of a privacy or security control.

Alternatively, or in addition, a risk based regulatory approach could allow AI developers to conduct and register an AI risk assessment for their technology for certain specified use cases. Deployers could then rely on the pre-existing risk assessment, provided their use remains within the bounds of the risk-assessed use case.[30]

We would not support a full exemption from risk-management requirements for small businesses, as their capacity to cause harm through poorly considered deployment of AI is not materially different to any other business.

17. What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?

elevenM position	The following additional elements should be considered as part of a risk-based approach: • system security; • traceability, access and audit logging; • empirical performance testing; • a right to opt-out; and

[30] The UTS Human Technology Institute's Facial Recognition Model Law proposes a similar approach for facial recognition technology impact assessments – see *HTI FRT Model law*', above n 5, page 62.

- registration with a regulator.

We support the Human Technology Institute's Model Law approach for facial recognition technology in law enforcement and national security.

The following additional elements should be considered as part of a risk-based approach:

- System security:
  - Security standards for AI systems and their implementations should be commensurate with the likely consequences of compromise.
- Traceability, access and audit logging:
  - It may be appropriate to require higher risk systems to retain logs of their activity for a minimum period for auditing purposes.
- Empirical performance testing:
  - Developers and deployers proposing to use AI for a high risk activity should be expected to be able to empirically demonstrate its effectiveness. Performance testing may be particularly useful for managing certain types of risk, for example discrimination risk with respect to facial recognition, which may perform differently in relation to different demographic groups.
- Right to opt-out:
  - Providing individuals with a right to opt-out of automated decision-making processes is an important control to address individual concerns. Opt-out rights may be appropriate in some circumstances where the scale and speed of the AI application does not allow human in the loop for all cases.
- Registration and approval:
  - There may be a case for requiring registration or central review and/or approval of certain very high-risk applications such as in healthcare or automotive industries. Registration and review may also be appropriate in contexts where each application of a technology may be lower risk, but the cumulative impact of many applications may present systemic or cumulative risk. For example, where automated agents may interact with each other in rapid and unexpected ways.[31]

Additional controls should also be considered for law enforcement and national security deployments of AI, and in particular facial recognition. We support the Human Technology Institute's Model Law approach for facial recognition technology in law enforcement and national security.

18. How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?

elevenM position	Risk-management is well understood and will not require companies to 're-invent the wheel' by creating new, AI-focused compliance structures.

[31] For example, high frequency and algorithmic traders have caused extremely rapid price fluctuations in financial markets as a result of algorithmic interactions. See, e.g., Will Kenton, 'Flash Crash: What they are, causes, history', *Investopedia* (online), 1 April 2022, available at https://www.investopedia.com/terms/f/flash-crash.asp.

	While there may be substantial overlap between AI risks and privacy risks, we recommend against regulating AI solely through the lens of 'privacy'.

Risk management is an established field, well understood and operationalised by industry and government. Framing AI regulation in the language of risk will allow regulated entities to incorporate AI risk management into existing enterprise risk management frameworks with minimal disruption and a lower cost of compliance than trying to come up with a sui generis approach.

We recommend against regulating AI solely through the lens of 'privacy' law. Although personal information is often used in AI systems, privacy and AI risk are different things. Australia's *Privacy Act* regulates the use and misuse of 'personal information'.[32] AI systems may impact privacy:[33] for example, widespread deployment of facial recognition technology has significant implications for individual privacy.

However, the potential risks of AI systems go far beyond privacy. For example, AI systems trading on financial markets may lead to market instability,[34] Generative AI systems may lead to increased security risks[35] or more general threats to public discourse by streamlining the production of misinformation and disinformation.[36]

19. How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?

elevenM position	A risk-based approach should apply to general purpose AI systems by: • requiring system developers to anticipate use cases and assess their respective risks; and • by requiring system developers to provide sufficient information about their AI system to allow prospective deployers to reasonably assess the risk of any given use case.

System developers should assess foreseeable use cases

In many cases general purpose AI systems are offered as services (e.g., OpenAI). This means that organisations have visibility and control (both contractual and practical) over the permitted use cases. We suggest that an obligation to conduct a risk assessment against permitted use cases could be combined with a requirement for general purpose AI system developers and vendors to conduct regular systematic risk assessments to consider the impacts of the widespread deployment of their technologies. Both risk assessments should

[32] Though the conception of privacy as a human right is broader than that.
[33] In the sense of use and misuse of 'personal information'.
[34] See Kenton, above n 31.
[35] Jim Chilton, 'The new risks ChatGPT poses to cybersecurity', *Harvard Business Review* (online) 21 April 2023, available at https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity.
[36] Tiffany Hsu and Stuart A Thompson, 'Disinformation Researchers Raise Alarms About A.I. Chatbots', *The New York Times* (online), 8 February 2023, available at https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html.

consider the access model being offered to users by the system developer, the range of use cases that are permitted and the extent of the system developer's ability to detect and prevent misuse. Vendors should also be required to continually assess the use of their AI systems and identify new and novel risks emerging from new use cases.

System developers should provide sufficient information for deployers to assess risk

As discussed at question 9 above, risk management by deployers of AI systems will require model developers to provide meaningful transparency around model inputs and performance. Regulation should seek to secure a degree of business-to-business transparency to enable effective risk assessment and management.

20. Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:

a. **public or private organisations or both?**

b. **developers or deployers or both?**

elevenM position	Risk-based regulation should be mandatory and should apply to both deployers and developers in both public and private organisations.

Evidence shows that self-regulation is largely ineffective at changing behaviour. The Human Technology Institute recently published a report on *The state of AI governance in Australia*, which provides a succinct overview:

> *Empirical research indicates that AI principles and codes of ethics have little discernible impact on the behaviour of engineers developing AI systems … other research indicates that poorly-designed normative frameworks that rely on moral encouragement can be counterproductive, inducing precisely the behaviour the organisation wanted to avoid. …*
>
> *The ineffectiveness of AI principles on their own is supported by experience in other areas of corporate governance. Evidence from the work health and safety field indicates that regulations, inspections, prosecutions, guidance material, campaigns and enforceable undertakings are the most important incentives for businesses to adopt practices that keep workers safe. Relying on voluntary action, public pressure or outside incentives has little impact on behaviour.*[37]

We have argued throughout this submission that AI regulation should be focused on building trust in AI systems by managing risk and ensuring AI development and use is well aligned to community values and expectations.

This regulation must apply to public and private organisations and address all sources of risk across the AI supply chain, including developers and deployers of solutions. It needs to allow

[37] Lauren Solomon and Nicholas Davis, 'The State of AI Governance in Australia' (Report, Human Technology Institute, The University of Technology Sydney, 2023), available at https://www.uts.edu.au/human-technology-institute/news/report-launch-state-ai-governance-australia.

flexibility in some areas (which can be achieved with a risk-based model) and be more stringent in others (such as banning activities with the potential to cause real harm to people). The regime must be consistent with emerging international standards and it must be overseen by a well resourced and active regulator. In short, this regime must have teeth. Neither self-regulation nor limited focus on certain AI supply chain participants will deliver the consistency and reliability of outcome required to build public trust and drive adoption of new AI technologies.

Contributors

Jordan Wilson-Otto · Principal · LinkedIn

Jordan is an expert in privacy regulation, policy development and program management, with deep experience in privacy compliance, regulatory investigations, public policy, and open data. Since joining elevenM Jordan has managed complex privacy project development and implementation and helps our clients ensure they are at the forefront of privacy practice and compliance. Prior to elevenM, he was Assistant Commissioner for Operational Privacy and Assurance at the Office of the Victorian Information Commissioner, where he established and led the investigations and assurance function. Jordan has held leadership roles at GovHack and the Victorian Society for Computers and the Law, and holds a Bachelor of Laws and a Master of Laws from University of Melbourne.

Arjun Ramachandran · Principal · LinkedIn

Arjun is elevenM's communications lead and specialises in providing strategic advice and communications expertise to help organisations build trust in their cyber security and privacy programs, internally and externally. He has extensive experience in crisis communications, board and executive engagement and training, and advising organisations in how to embed privacy and cyber security culture. Arjun worked as a journalist at the Sydney Morning Herald and in senior media relations roles across government and the private sector before establishing the cyber outreach and advocacy program for the Commonwealth Bank of Australia, leading the bank's cyber security strategy, incident response communications and security awareness programs. Arjun holds a Master of Arts in Journalism and a Bachelor of Information Technology from the University of Technology, Sydney.

Melanie Marks · Principal · LinkedIn

As privacy practice lead of elevenM, Melanie works with Australia's most prominent brands to drive innovation and manage privacy and data governance risks. In the field for almost 20 years, Melanie brings deep expertise and knowledge to clients at all stages, from start-ups to large corporates. She is also committed to training the next generation of privacy professionals. Prior to elevenM, Melanie ran privacy governance programs for CBA and the National eHealth Transition Authority. She is a former President of the International Association of Privacy Professionals in the ANZ region, served on advisory boards for Information Governance ANZ and Hello Sunday Morning and is an Expert Advisor to LexisNexis on privacy and data protection. Melanie holds a Master of Industrial Property Law from the University of Technology, Sydney, a Bachelor of Media (Hons) and a Bachelor of Laws from Macquarie University. She is a Graduate of the Australian Institute of Company Directors.

Georgia Potgieter · Senior Consultant · LinkedIn

Georgia is a privacy specialist and admitted solicitor with a background in plaintiff litigation and crisis management. Georgia's professional experience has been in providing strategic guidance on privacy and data protection to organisations, including advice on contractual and regulatory obligations in the aftermath of a data breach. Prior to joining elevenM, she

worked at Slater and Gordon on the Optus and Medibank data breach class actions, as well as providing advice on risk, notification obligations, and multi-jurisdictional compliance. Georgia holds a Bachelor of Laws and a Bachelor of Arts (Media, Culture, and Communications) from Macquarie University and is currently completing a Master of Administrative Law and Public Policy at the University of Sydney.

Angela Wong · Senior Consultant · LinkedIn

Angela is a privacy specialist with over a decade of experience in privacy regulation and communications. Prior to joining elevenM, Angela spent ten years at the Office of the Australian Information Commissioner (OAIC), working as a solicitor in the legal team and, prior to that, in the communications team. Angela has extensive experience in regulation and compliance, the development and implementation of privacy processes, and privacy and security awareness activities.

Nick Dyson · Consultant · LinkedIn

Nick is a privacy consultant with a background in technology and legal non-profits. Nick has a passion for the intersection between law and technology and is a member of the Australasian Cyber Law Institute, serving on several committees including the Cyber and Human Rights Committee. He is also currently the president of the Victorian chapter of The Legal Forecast. Nick holds a Bachelor of Laws (Hons) and a Bachelor of Commerce (Finance) from La Trobe University.

Jonathan Gadir · Senior Consultant · LinkedIn

Jonathan is a privacy specialist with experience spanning media, consumer law, financial services and technology. A former journalist and lawyer, he moved into regulatory policy, working for Australia's peak consumer organisation. He has authored many submissions to government and represented consumers before parliamentary committees and at international forums. Jonathan has held policy roles in New South Wales state government agencies including Department of Finance, Services and Innovation and Cyber Security NSW and most recently, operational privacy roles at IAG and AMP.