Human Technology Institute

INSIGHT SUMMARY

ASIC x UTS: AI Regulators Symposium

21 May 2024

Insights from the ASIC x UTS: AI Regulators Symposium

This summary presents a range of perspectives from participants to the AI Regulators Symposium hosted by ASIC and the UTS Human Technology Institute (HTI) on 21 May 2024. The symposium included public panels featuring several leading Australian regulators and a roundtable discussion with 40 AI thought leaders under the Chatham House Rule. Accordingly, the content of this summary should not be held to represent the views of ASIC, HTI or any specific participants.

The purpose of the symposium was to explore the conditions necessary for the effective regulation of AI through discussion grounded in practical examples.

1

While there are clear gaps in legislation and an opportunity for law reform, the effective application and enforcement of existing laws can address many of the harms arising from AI systems.

2

Although regulators would be better supported by law reform and additional resourcing, they can provide guidance, undertake enforcement action, and coordinate with other regulators on AI-related issues.

3

Australia can play a leadership role in the protection and enforcement of people's rights in response to harms caused by the deployment of AI systems.

TLDR: A quick summary of what we heard

Application and reform of laws

- **Current laws:** There is no 'AI wild west'; about two-thirds of AI harms are covered by existing laws. However, barriers exist to their effective application and enforcement.
- **Law Reform:** To address the full range of AI harms, law reform is necessary, particularly modernising Australian privacy laws. Law reform should be undertaken through extensive consultation between government, industry, civil society, and the community.
- **Accountability:** Companies and directors should be accountable for AI-supported decisions, or else corporate liability for AI may need to be reformed.
- **Guidance and clarity:** More guidance is needed on how current laws apply to AI. This could be provided by regulators through formal guidance or enforcement actions. A lack of legal clarity can lead to increased regulatory burdens and overcompliance, especially for SMEs.

Regulators' role and requirements

- **Impact of AI:** Regulators are using AI to support staff and assist with their investigative functions. AI is creating new harms, enhancing existing ones, and challenging traditional enforcement strategies for regulators.
- **More resources:** Effective AI regulation requires strong enforcement by well-resourced and skilled regulators. More resources would support regulators to bring enforcement actions and strengthen their AI expertise by upskilling and hiring more technical staff.
- **Regulator coordination:** Coordination among regulators is crucial, both domestically and internationally, to address intersecting AI-related issues and the market power of overseas AI developers.
- **Supporting actions**: Regulators need to be supported by other mechanisms, such as class actions, to clarify laws and address problems at scale. With additional resources, civil society could help identify and run test cases.

Australian AI leadership

- **Encouraging adoption:** AI adoption and innovation would be encouraged by safeguards that manage risks and secure benefits.
- **AI deployer:** Australia is primarily a deployer of AI, not a developer. Participants felt Australia should not aim to introduce the first or most stringent AI regulation.
- **Balanced regulation:** Australia could lead in AI regulation through a mix of hard and soft regulatory responses, such as supporting good governance, targeted law reform, regulatory guidance, and strong enforcement against AI harms.
- **Ongoing journey:** It will take time to see which international AI regulation approaches are effective. Strict regulation lacks flexibility, whilst a focus on good governance allows for more experimentation. Participants supported the collaborative development of governance models and tools by government, industry and civil society.

Opening remarks

Joseph Longo, Chair, Australian Securities and Investment Commission

'We should avoid… the notion that AI is too complex to be knowable. Like all technology, AI is the product of human ingenuity and can therefore, by definition, be understood. Moreover, it is the job of government and regulators to ensure that these systems are explainable and transparent …

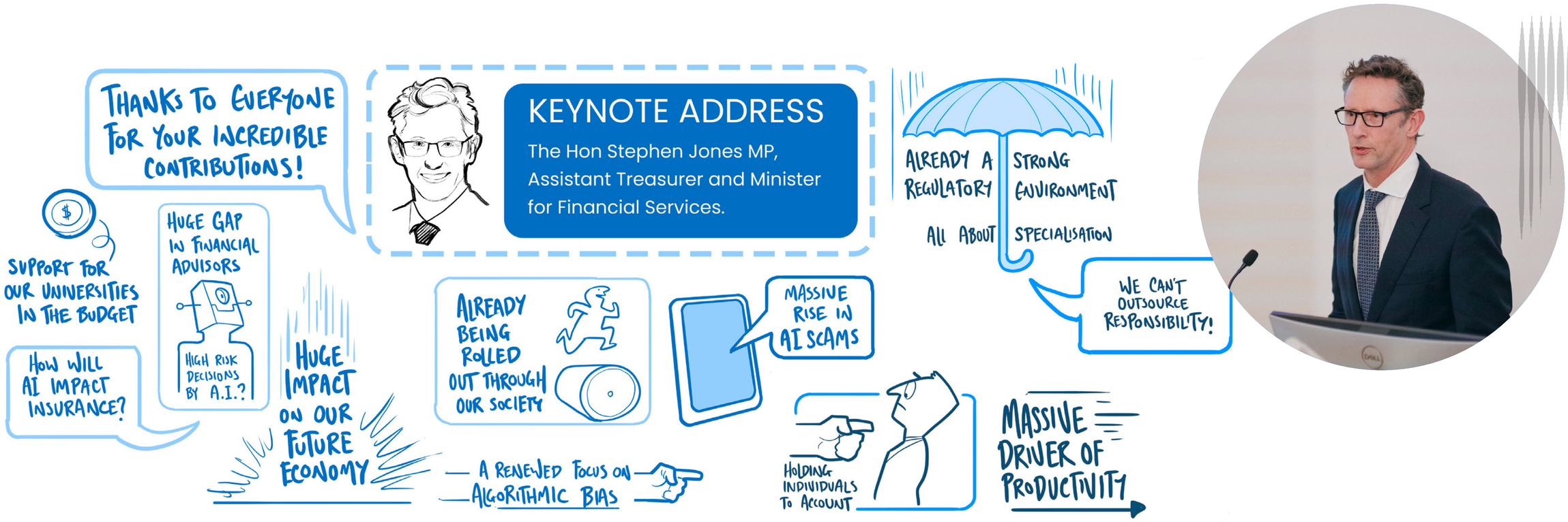
Across Australia, a consensus is developing: we need a strong regulatory framework to steer the course of AI towards its safe and responsible development and use. A framework that enables technological innovation to flourish, so that it can deliver the promised economic benefits and productivity improvements. But not at the expense of consumers and investors.'

Keynote address

The Hon Stephen Jones MP
Assistant Treasurer and Minister for Financial Service

'Across just about every area of our law… we attach responsibility for decisions to people, to directors, to corporate entities, to responsible persons inside organisations… to licensees, and those decisions cannot be outsourced to a machine or anything else…

We will continue to hold corporate people and real people responsible for the decisions whether they are made by them or whether at some point in the decision-making process it is built on information that is provided to them by AI machinery.'



01.

Insights from AI regulators

‘Our job is to mitigate the known risks – and, in doing so, bend the trajectory away from the worst imagined outcomes, so that they never materialise.’

ASIC Chair, Joe Longo

Regulators panel

21 May 2024 | 18.30-19.30

Panel members:

Liza Carver
Commissioner, Australian Consumer and Competition Commission

Julie Inman Grant
eSafety Commissioner, eSafety Commission

Carly Kind
Privacy Commissioner, Office of the Australian Information Commissioner

Joe Longo
Chair, Australian Securities and Investment Commission

Facilitator:

Professor Nicholas Davis
Co-Director, Human Technology Institute, UTS

Key insights:

- AI is being deployed by regulators to assist support staff and their investigative and enforcement functions.
- AI is impacting all regulators by creating new sources of harms and 'turbocharging' existing ones. Many of these issues overlap, and regulators are aware of the need to work together to coordinate their responses to AI harms.
- AI is challenging traditional enforcement strategies for practical reasons (e.g. scale and accessibility of AI technologies; consumers are unaware of rights or breaches, but the burden is on them to bring complaints) and legal reasons (e.g. uncertainty around liability for AI systems; application of Australian laws to foreign developers who dominant the market).
- Regulators need more resources. They need additional financial resources to investigate and bring enforcement actions, but they also need to strengthen their AI expertise by upskilling staff and hiring more staff with technical experience.

ASIC X UTS: AI REGULATORS SYMPOSIUM

IMPORTANCE OF EDUCATING THE PUBLIC

HOW CAN REGULATORS COLLABORATE MORE?

GENERATIVE AI

E-SAFETY JUST GETTING STARTED

THE OPPORTUNITY TO HELP WITH THE VERY HARD WORK OF E-SAFETY

DOMINANCE OF THE MAJOR PLAYERS IN AI

WHAT IS THE FUTURE OF LEGAL LIABILITY?

E-SAFETY STARTING TO COME TO AGE

ARE THE CREATORS OF THE MODELS RESPONSIBLE?

DANGERS + OPPORTUNITIES OF OPEN SOURCE MODELS

FEARS OF SYSTEMS WITHOUT GUARDRAILS

LOCAL IMPACTS OF A GLOBAL ISSUE

WE HAVE TO KNOW WHERE OUR DATA IS FROM

ONLINE SAFETY CORRELATIONS WITH HUMAN RIGHTS

AI REGULATION IN AUSTRALIA TODAY

Joseph Longo – Chair, ASIC

Julie Inman Grant – eSafety Commissioner

Carly Kind – Privacy Commissioner

Liza Carver, ACCC Commissioner

HOW CAN WE PROTECT CONSUMERS

NEW WAYS TO IDENTIFY RISKS NEEDED

HARMS FELT COLLECTIVELY

ABILITY TO PROTECT AND CARE FOR THE MOST VULNERABLE WITH AI

DESIRE FOR CLEAR REGULATORY GUIDANCE

GREAT POTENTIAL THREAT TO OUR SOVEREIGNTY

DANGERS OF ERRODING TRUST

FORENSIC CAPABILITIES OF AI

DANGERS OF OUT OF CONTROL DEEPFAKES

NEED FOR SCIENCE RETRAINING IN THE INDUSTRY

MORE RESOURCES FOR REGULATORS!

DATA IS THE FEEDSTOCK OF AI

How is AI impacting regulators?

How are regulators using AI?

- AI is being used as an investigative and enforcement tool, including for document review, monitoring online commercial activity, analysing market trends and detecting technology-facilitated abuse.
- Machine-learning systems are being used to protect staff. For example, image masking is supporting eSafety staff who are required to review disturbing material (e.g. child abuse, terroristic material).
- AI is not eliminating human involvement in regulatory activities – there is always a human in the loop.

What harms or issues are regulators seeing?

- AI has turbocharged consumer harms (e.g. scams) and is impacting privacy and data rights.
- Personal data is the feedstock of AI. Technology companies are incentivised to own data to entrench their position in the AI market, or to monetise it by licensing to other firms to train their AI systems.
- There are market collusion, anti-competitive and jurisdiction issues in relation to AI foundation models as they are created and hosted outside of Australia.
- Companies need to put in place effective data governance and manage supply chain vulnerabilities relating to AI systems.

What are the challenges of AI for regulators?

- Regulatory action, and resource allocation, is driven by individual complaints. Yet, harms are occurring at both the collective and individual level. The opacity of AI is also creating challenges. For example, individuals are not always aware of privacy violations caused by AI systems. As such, the OAIC is trying to detect privacy breaches through other investigatory methods (e.g. puppet audit, mystery shopper investigation).
- AI issues can intersect with multiple regulatory regimes, requiring cooperation between regulators. For example, there is overlap between the OAIC and ACCC's work on digital platforms and data brokers.
- Given the growth and scale of AI, regulators will need additional resources to bring enforcement actions. Regulators also need to build their technical expertise and upskill their legal and policy teams.
- Companies and directors cannot delegate their decision-making authority and responsibility to AI. There may be a need for law reform around corporate liability for AI.

What more do regulators need to regulate AI?

What regulatory reforms are needed?

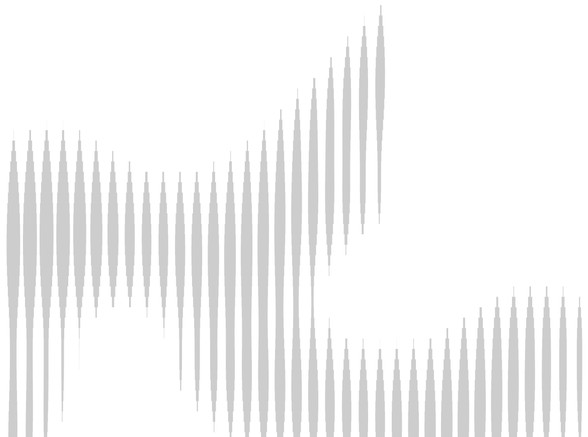
Regulators highlighted the following:

- **Modernisation of privacy laws and data rights:** Targeted privacy and competition law reform is needed to address systemic, non-compliant behaviour by digital platforms expansively collecting user data.
- **Reforms to address social harms:** Reforms are needed given the increasing accessibility of sophisticated AI systems that can be used to cause harm or misled (e.g. deepfakes).
- **Regulatory coherence:** Governments and regulators need to coordinate domestically and internationally to address AI issues. International cooperation needs to be grounded in the reality of how technology companies operate and where they are domiciled.

What else is needed?

Regulators said that:

- Regulators need additional resources to upskill, provide guidance, and undertake investigations and enforcement actions.
- Greater investment in civil society would help such organisations to identify legal test cases for real-world harms of AI systems that could ground regulatory enforcement actions. This investment could be financed by a stronger penalty regime.
- Individuals need assistance and support mechanisms to connect them with regulators with the best fit and remit for their AI-related complaints.
- The standardisation and simplification of terms and conditions (T&Cs) relating to data would help consumers understand how their personal information is being used. The average consumer would currently need to spend 45 hours per month reviewing product T&Cs.



02.

Insights from AI thought leaders

‘Australia can be a world leader in designing a nuanced approach to AI regulation’

Roundtable participant

AI thought leaders panel

21 May 2024 | 18.00-18.30

Panel members:

Anna Jaffe
Director of Regulatory Affairs & Ethics, Atlassian

Lizzie O'Shea
Chair, Digital Rights Watch

Professor Ed Santow
Co-Director, Human Technology Institute, UTS

Facilitator:

Professor Nicholas Davis
Co-Director, Human Technology Institute, UTS

The panel shared the following key insights from the roundtable:

- Regulation needs to address the full spectrum of AI-related harms with corresponding remedies from the individual level to the systemic level.
- Effective regulation of privacy and data is foundational and antecedent to effective AI regulation. Privacy law needs to be modernised to account for AI, incentivise good use of data, and strengthen the data rights of individuals.
- The institutionalisation of civil society engagement is needed to establish meaningful feedback loops to identify AI-related problems before they manifest at scale and mitigate the worst excesses of irresponsible AI usage. Organisations should see the value of community input to improve their system.
- Law reform around AI, as well as stronger powers for existing regulators to enforce those laws, is necessary but insufficient to uplift the regulatory ecosystem to address AI. Regulators will also require greater technical capabilities and resources to access and make sense of the relevant information around AI – recruiting technologists will be key.

What can we learn from international regulatory approaches?

Other reflections from the panel:

- Different jurisdictions approach AI regulation differently depending on the structure of their economy, national values and priorities. Australia is positioning itself as an adaptor rather than innovator of AI which may affect its approach.
- A mixture of hard and soft law provides flexible adaptability to respond to the rapid developments of AI. Regulation that is too rigid will struggle to meet the fast-paced growth of AI (as the EU encountered with the explosion of generative AI). However, as the EU has done, some roundtable participants suggested that some AI uses should be banned based on prescribed criteria
- In both Australia and overseas, regulatory guidance is needed to address current uncertainty around how existing laws apply to AI.
- Regulatory action needs to be supplemented by other mechanisms to effectively enforce laws and remedy problems. For example, class-actions are critical for remedying harms at scale, which can be beyond the scope of regulators who focus on individual complaints.

AI thought leaders roundtable

21 May 2024 | 14.30-16.30

40 regulatory, industry, civil society, legal, and technical experts explored three key topics:

1

Existing laws:
How do they address AI harms? How do we ensure the effective application and enforcement of existing laws?

While gaps exist, current laws can address many harms from AI systems. However, there are significant barriers relating to enforcement.

2

Emerging AI use cases:
What are the new and emerging use cases where there is a gap in the law or regulatory powers?

Participants saw the ability of AI models to mislead and manipulate consumers as a significant concern and area for regulatory attention.

3

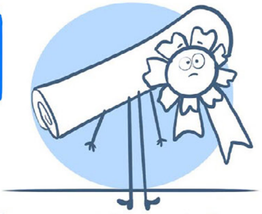
International regulation:
What can Australia learn from international regulatory models or approaches? How can Australia lead in the regulation of AI?

Australia can learn from different approaches with focus on improving AI governance. Leadership will need investment in law reform, guidance and enforcement.

AI THOUGHT LEADERS ROUNDTABLE

WELCOME TO UTS!!

FOCUSSING ON THE HOW OF FUTURE AI POLICY



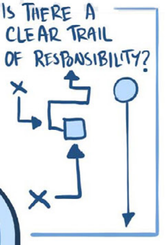
LACK OF LEGAL CERTAINTY = MAIN CONCERN

WHAT NEEDS TO CHANGE FOR THIS PROBLEM TO BE ROUTINELY SOLVED?

CAN WE HAVE MORE TRANSPARENT TERMS OF SERVICE?

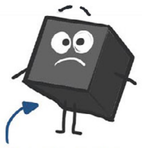
CAN CONSUMERS SEE DOWN-STREAM CONSEQUENCES?

IS THERE A CLEAR TRAIL OF RESPONSIBILITY?



A CLEAR INTERNAL DISPUTE RESOLUTION PROCESS?

HOW CAN THE CONSUMER FEEL LIKE THEY ARE BEING TREATED FAIRLY?



ADDRESSING THE BLACK BOX ISSUE

IS THE RESPONSIBILITY WITH THE REGULATOR OR WITH THE SUPPLIER?

A FIT FOR PURPOSE DISPUTE RESOLUTION PROCESS

ARE WE ADEQUATELY STRESS TESTING OUR ORGANISATIONS

FAST CASH CASE STUDY

- REGULATORY POWERS COVER CURRENT REGULATION

BUT THEY ARE HARD TO PROSECUTE!

GOOD REVIEWS OF UK POLICY

WHAT CAN WE LEARN FROM MISTAKES GLOBALLY?

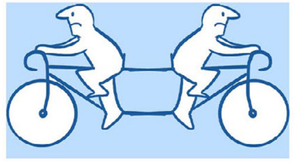
BAD REVIEWS OF EU POLICY

WHAT DO YOU WANT TO SEE PRIORITISED?

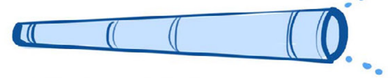
SHOULD AUSTRALIA POLICE DEVELOPMENT OR JUST CONSEQUENCES?

IS THERE A GAP IN LAW OR REGULATORY POWERS?

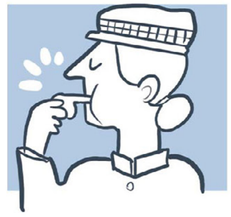
ARE THE REGULATORY SERVICES WORKING IN TANDEM?

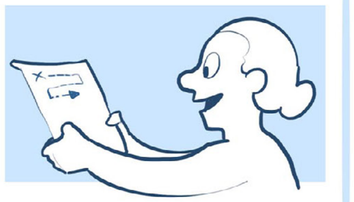


SHOULD WE FOCUS ON DETAIL OR SCOPE?



CAN WE FINALLY GET A DIGITAL PLATFORM OMBUDSMAN?





CONSUMER EXPLAINABILITY?

WILL PROVIDORS OPEN UP THEIR SYSTEMS?

GOOD GENERALIZED LAWS NEED TO COME FIRST

HOW DO WE DEFINE "HARM"?

WHAT ARE THE BROADER IMPLICATIONS OF AI

WHAT IS 'REASONABLE' EXPLAINABILITY

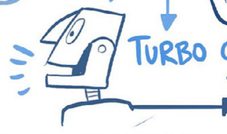
THE LONG SHADOW OF ROBO-DEBT

SYSTEMS VS HUMAN ERROR

DIFFERENT GLOBAL LEGAL ENVIROMENTS

CONSUMERS NEED SOMEWHERE TO GO TO RESOLVE DISPUTES

THINKING ABOUT THE POWER OF A.I. PERSUASION



TURBO CHARGING

INFORMATION WARFARE

"THE GRADUAL SUPRESSION OF HUMAN FREE WILL"

HOW MUCH CAN WE RELY ON CONSUMER REPORTING?

MORE AI TRANSPARENCY!

TURN OFF THE TAP!

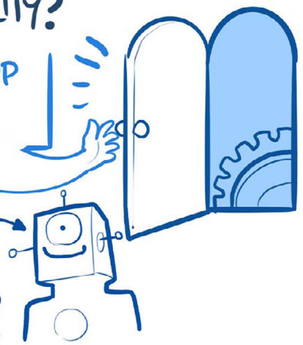
LOOKING AT THE BROADER DATA ECOSYSTEM

WHAT IS WITHIN OUR SCOPE OF CONTROL?

SYSTEM FAILURE VS HUMAN FAILURE

CAN WE EVER MOVE FAST ENOUGH?

CAN WE EVEN CATEGORIZE THE PROBLEM AT HAND?



WHAT KIND OF AI ARE WE TALKING ABOUT?

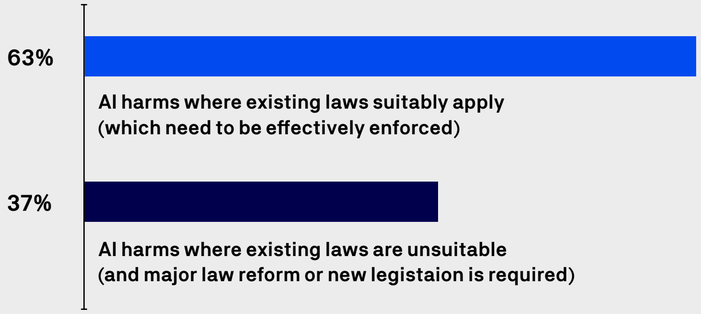
How do existing laws apply?

A case study (see page 21) was used to practically ground the discussion around the question of how existing laws and regulatory powers apply to the use of AI systems and address their potential harms.

Participants discussed a wide range of existing laws and regulatory powers that are relevant and applicable to situations where consumers are harmed by AI systems such as:

- Privacy laws;
- Australian Consumer Law;
- Corporations law (including directors' duties and AFS licensee obligations);
- APRA standards;
- consumer credit protections; and
- anti-discrimination laws.

There is no 'AI wild west'. Many AI harms or issues are addressed by current laws, according to participants when asked what they perceived to be the proportion of AI harms or issues that are suitably covered by existing Australian laws:



Addressing the remaining harms will require major law reform. Participants identified a range of significant barriers to the effective application and enforcement of existing laws.

Will existing laws address AI harms?

Although there are applicable laws and regulatory powers, these are not always effectively applied and utilised. Participants discussed the challenges of applying existing laws and how to overcome them.

Participants identified various challenges including:

- regulators need more resources to upskill, investigate and bring enforcement actions;
- overlapping responsibilities between regulators can create uncertainty or delay in actions;
- the burden of bringing claims is on individuals, who may not be aware of their rights, the breaches, or have the resources to bring ac claim;
- there are legal and practical difficulties in enforcement actions (i.e. gathering the necessary evidence, establishing causation, liability, loss, damages); and
- there is some uncertainty as to how the law applies to AI systems.

To respond to these challenges, participants highlighted a need for:

- updated guidance by regulators, including joint guidance;
- class actions that enforce and clarify the rights of consumers;
- transparency and disclosure to consumers where they are affected by a decision made by AI systems;
- clarity on the question of liability where organisations claim that they delegated responsibility to an AI system; and
- stronger, enforceable penalties for organisations that breach the law to deter bad behaviour.

Ranking the barriers to effective regulation

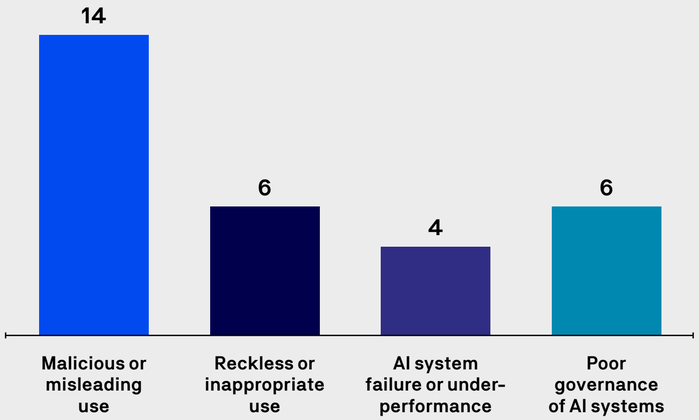
Participants were asked to rank the factors they felt were the biggest barriers to addressing AI harms in Australia today.

Emerging AI use cases and sources of AI harms

Participants were concerned about AI being used in the following contexts where they felt there was a gap in existing laws or regulatory powers:

- targeting and influencing people through conversational approaches;
- spreading misinformation and disinformation;
- surveillance and tracking, particularly being used by perpetrators of domestic violence against their victims;
- administrative decisions by governments;
- facial recognition technology; and
- neurotechnology.

Participants were also asked what causes of AI harms they worry about the most (see results below). Many of these emerging use cases fall into the category that participants were most concerned about, being the malicious or misleading use of AI systems.



International regulation

Participants were asked what Australia can learn, either positively or negatively, from international AI regulatory approaches. The following approaches were highlighted:

EU

Participants considered the EU's comprehensive AI law to be a critical development, but also problematic given the challenge of directly regulating AI.

UK

Many participants agreed with UK's approach of greater central greater central coordination, collaboration, and oversight by existing regulators.

Switzerland

Some participants suggested that, like Switzerland, Australia should first understand how existing laws apply and identify gaps before making reforms.

Singapore

Participants also pointed to the Singapore's government support of AI governance frameworks and tools for industry as an example for Australia.

What other lessons are there for Australia?

- Risk-based approaches, tech-neutral or principles-based legislation, and operationalization of ethical principles by industry supported by majority of participants.
- AI regulation is an ongoing journey. It will take time to see which approaches are effective.
- Strict regulation does not provide flexibility. Focusing on implementing good governance allows for greater experimentation by organisations.
- There is a risk of overcompliance by, and increased regulatory burden on, SMEs and NFPs when there is uncertainty on the application of new laws.
- To date, there has been insufficient consultation with experts, civil society, and the community on the development and regulation of AI systems.
- Coordination across government and between regulators is needed.

How can Australia lead in AI regulation?

What does it mean for Australia to lead in AI regulation? Participants said:

- Australia is primarily a deployer of AI, not a developer. Some participants noted that Australia should not strive to be first to introduce regulation, nor to introduce the most stringent regulation;
- regulation needs to provide protections for impacted communities without creating significant regulatory burdens; and
- AI adoption and innovation will be encouraged in Australia through the development of effective safeguards that manage the risks and secure the benefits of AI systems.

To lead, participants suggested that Australia needed:

- law reform (particularly privacy laws) to address AI harms developed through widespread consultation;
- more investment in research and development, the regulatory framework and regulators in order to protect Australians and their data;
- better guidance and education on the application of current laws to AI;
- governance models, tools, and standards developed through collaboration between industry, government and civil society; and
- strong and effective enforcement of laws by well-resourced and skilled regulators.

Appendix 1

FastCash case study

To ground the discussion in a practical example, participants were provided with this case study in advance of the symposium.

Company FastCash Loans is a provider of financial services and credit licence holder, with a turnover of over $50 million per year. FastCash has begun combining previously screen scraped banking data with other non-financial consumer data it collects for a range of purposes about potential consumers via a data matching process with data it receives from data broker GiantEye. FastCash Loans does not know how GiantEye collected the detailed data it shares about consumers and does not have any way of ensuring that this has been collected legally, nor does it have complete certainty on whether the data is accurate.

FastCash Loans is using an AI-powered credit assessment tool provided by a third party to analyse this data and make automated decisions about product suitability based on revenue optimisation. This process is helping to speed up lending decisions and responses to loan applicants, as well as supporting FastCash Loans to deliver increasingly sophisticated price discrimination techniques to target consumer loans to each individual consumer. Unbeknownst to FastCash Loans, the combined data used to train the AI credit assessment tool was recently subject to a data poisoning attack, producing incorrect product suitability assessments.

Consumer Vihaan Anad is a recent migrant living in a regional area. He applies with FastCash Loans for a loan to cover the costs of an upcoming urgent medical operation for his daughter, consenting to the use of data held by GiantEye for the purpose of providing him with a tailored lending offer. Within 24 hours, Vihaan receives an automated email saying that he is not eligible for the loan. Vihaan is not aware of why this decision was made, but asks for clarification from FastCash Loans, who in turn responds with ‘our credit assessment tool deemed you ineligible for this product’. Vihaan asks for a review of the decision, believing he has been unfairly discriminated against, underscoring the urgency of his situation. This complaint is taken up by an internal FastCash Loans Customer Advocate who checks the process for how a decision was reached. The Customer Advocate is not able to interrogate how or why the assessment tool determined Vihaan’s suitability but advises the customer of the types of data that have been used to make an assessment and confirms that Vihaan remains ineligible.

Human Technology Institute

For more information on HTI's AI Corporate Governance Program, or to join our AI Governance network, please contact:

Llewellyn Spink, AI Corporate Governance Specialist
llewellyn.spink@uts.edu.au

UTS CRICOS 00099F