NSW Council for Civil Liberties Inc.
PO Box A1386, Sydney South,
NSW 1235, Australia

e: office@nswccl.org.au
t: 02 8090 2952
www.nswccl.org.au

@nswccl
@nswccl

NSWCCL SUBMISSION

THE DEPARTMENT OF INDUSTRY, SCIENCE AND RESOURCES

SAFE AND RESPONSIBLE AI IN AUSTRALIA – DISCUSSION PAPER

26 July 2023

Acknowledgement of Country

In the spirit of reconciliation, the NSW Council for Civil Liberties acknowledges the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all First Nations peoples across Australia. We recognise that sovereignty was never ceded.

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

1. EXECUTIVE SUMMARY

The NSW Council of Civil Liberties (**NSWCCL**) submits that the proliferation Artificial Intelligence (**AI**) poses significant risks to the civil rights of the Australian public. As it stands, Australia's regulatory system fails to fully address these risks – an issue that will grow with increased use of these technologies.

The proceeding submission responds to the key questions of concern for the NSWCCL from the Discussion Paper. In this submission the NSWCCL, recommends that:

1. A statutory office of an AI Safety Commissioner be introduced, to lead regulation and research of new AI risks and coordinate responses of different government bodies and agencies;

2. Reform the existing patchwork of legislation that covers AI regulation, including improved privacy protections for citizens;

3. Introduce bespoke AI regulation that adopts a risk-based approach to AI, with graduated obligations for AI developers, deployers and users of AI according to risk. This should include:

    a. Transparency requirements for all deployers of AI, which become more onerous with the risk associated with the kind of AI;

    b. Distinct and more onerous transparency requirements for public sector organisations that use AI and ADM;

    c. Prohibitions on some kinds of AI use in decision-making (differing from private and public sectors);

    d. Flexibly-defined prohibitions on AI that poses an unacceptable risk of harm; and

    e. A regime that delegates specific compliance responsibilities for developers (of upstream and downstream applications), deployers and users.

Appended to our submission are the NSWCCL's previous submissions to the Department of Prime Minister and Cabinet's Digital Technology Taskforce[1] and the Commonwealth Attorney-General[2] on AI regulation and the *Privacy Act 1988* (Cth) respectively. These submissions are relevant to the Department's current inquiry, and we submit that the Department should also consider the recommendations outlined therein.

[1] NSWCCL, Submission to Department of the Prime Minister and Cabinet, Digital Technology Taskforce, 'Positioning Australia as a Leader in Digital Economy Regulation – Automated Decision Making and AI Regulation – Issues Paper' (20 May 2022) (**NSWCCL Submission to ADM and AI Regulation Issues Paper**).

[2] NSWCCL Submission to the Attorney –General's Department, Privacy Act Review – Discussion Paper (9 January 2022) (**NSWCCL Submission to Privacy Act Review**).

2. INTRODUCTION

The NSW Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Department of Industry, Science and Resources (the **Department**) in regard to the *Safe and Responsible AI in Australia – Discussion Paper* (the **Discussion Paper**).

AI poses profound risks to Australians' human rights. They have the potential to make important decisions that affect our lives in an automated way that is less open, fair and transparent. The growth of AI, both in terms of the technology that underpins it, and the ever increasing private and public sector applications, poses new risks to rights to privacy. For instance, sensitive personal information can be scraped for use in AI training, and AI can be deployed to track people in real-time through biometric identification systems or compile comprehensive consumer profiles. A key risk here is that AI systems can reproduce biases which, when coupled with the opaque nature of their decision-making, can be difficult to identify. Given the lack of transparency in the regulatory requirements for developers and deployers of AI and Automated Decision-Making (**ADM**) systems, many Australians will not be aware when they have come in contact with such systems.

Perhaps the most recent example of the pitfalls of poorly regulated ADM is the Robodebt Scheme, which highlights that the misuse of even simple kinds of ADM can lead to fatal outcomes for vulnerable Australians. As the Royal Commission into Robodebt has found, a simple form of ADM was deployed at large scale by the Department of Social Services to calculate "overpayments" made to welfare recipients.[3] Fundamental errors in the ADM led to miscalculation of welfare entitlements for thousands of vulnerable recipients and false accusations of overpayments.[4] While all Australians are potentially at risk of harm from the misuse of AI and ADM, Robodebt reminds us that poorer and marginalised communities will find it more difficult to assert their rights or seek redress. The NSWCCL urges the Department to keep such citizens front of mind when drafting its recommendations. Though the Robodebt Scheme did not involve AI, the growth of this technology (which is more complex and opaque than the simple ADM system Robodebt used) threatens similar harms. Appropriate procedural safeguards and review mechanisms that protect such people should be the hall marks of a responsible AI regulatory framework.

As noted in the Discussion Paper, AI offers significant opportunities to Australia. But these opportunities come with risks. Absent significant reform, the proliferation of these technologies will lead to abuses of rights to privacy, equality and fairness. The NSWCCL submits urgent reform to the existing patchwork of regulations that covers AI, to fill in gaps and address emerging risks. Specifically, we call for a bespoke AI regulation that adopts a risk-based approach, as well as the introduction of an AI Safety Commissioner that could oversee regulation in this increasingly important area.

3. FEEDBACK ON THE DISCUSSION PAPER QUESTIONS

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

NSWCCL sets out its comments below on certain the definitions of: (a) Artificial Intelligence; and (b) Automated Decision Making, as defined in the Discussion Paper.

(a) Artificial Intelligence

AI terms will be defined and used differently, depending on the context and goals – the goals of defining AI for scientific usage differ from the goals of defining AI for the purposes of AI legislation. To the extent that the definitions in this Discussion Paper are intended to flow through to legislation, the NSWCCL

[3] Royal Commission into the Robodebt Scheme (Report, 7 Jule 2023) Section 2.
[4] Ibid, xxiii – xxix.

submits that these definitions may be too narrow in scope and may not focus enough on the impact of AI technologies.

(i) Scope

The definition of "artificial intelligence" in the Discussion Paper is as follows: "*an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation*".

NSWCCL submits that this definition is amended to be: "*an engineered system that generates, for a given set of human-defined objects or parameters, predictive outputs, content, forecasts, recommendations or decisions that influence real and virtual environments. AI systems are designed to operate with varying levels of automation and autonomy."*

The NSWCCL supports the *focus* of the definition of "AI Systems" in the Discussion Paper for definition on predictive outputs, content, forecasts, recommendations, and decisions. However, we submit that the words "content, forecasts, recommendations or decisions" should sit alongside "predictive outputs", rather than being listed as a subset of those outputs. It is not clear even too technical experts how AI systems may develop or react, and "predictive outputs" may be too narrow. For example, large language models have shown "emergent abilities" that were not present in smaller models and thus could not be predicted simply by extrapolating from those smaller models.[5]

Additionally, the reference to "without explicit programming" may set too high a bar for the level of autonomy expected and could exclude AI systems with some explicit programming – rather, the definition should not include this and should recognise that AI systems can operate with varying levels of autonomy.

(ii) Impact

The Discussion Paper definition of AI Systems does not refer to the impact they can have. The NSWCCL submits that the appropriate scope and focus of AI legislation is on identifiable real-world systems with an impact on real or virtual environments.

We consider the definition of AI should not extend to all possible AI systems that may be developed, both present and future, including in the research domain.[6] The NSWCCL submits that legislation that has real world application and protects against undesirable consequences – such as in safety, health or human rights – while also allowing room for innovation in research to develop trustworthy AI offers the most effective, pragmatic approach that will also not stifle innovation in a nascent industry. In this respect, the NSWCCL submits that the Department should have regard to the following international guidance with respect to definitional focus on the impact that AI systems can have in terms of influencing real or virtual environments:

- The US *National AI Initiative Act of 2020* defines the term "artificial intelligence" as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action".[7] This is a definition has reference to underlying methodologies, but still refers to the impact of AI in that it "[influences] real or virtual environments".

[5] Wei et. al, 'Emergent Abilities of Large Language Models', *Transactions on Machine Learning Research* (August 2022), https://openreview.net/pdf?id=yzkSU5zdwD.
[6] Mireille Hildebrandt, "Global Competition and Convergence of AI Law" (2022) *SocArXiv 10* <https://doi.org/10.31235/osf.io/j36ke>.
[7] National Artificial Intelligence Initiative Act of 2020, DIVISION E, SEC. 5002, Article (3).

- In 2019, the OECD Recommendation of the Council on Artificial Intelligence adopted the definition of "AI systems" as follows: "An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy".[8] More so than the previous one, this definition focuses on the impact of the AI system with less focus on underlying methodologies, also referring to "influencing real or virtual environments".

- Finally, Article 3(1) of the proposed EU *Artificial Intelligence Act* (**AI Act**) defines "artificial intelligence system" as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". Again, the definition refers to "influencing the environments" that the AI system "[interacts] with".

(b) Automated Decision Making (ADM)

The Discussion Paper defines "Automated Decision Making" as a reference "*to the application of automated systems in any part of the decision-making process. Automated decision making includes using automated systems to:*

- *make the final decision*
- *make interim assessments or decisions leading up to the final decision*
- *recommend a decision to a human decision-maker*
- *guide a human decision-maker through relevant facts, legislation or policy*
- *automate aspects of the fact-finding process which may influence an interim decision or*
- *the final decision.*

Automated systems range from traditional non-technological rules-based systems to specialised technological systems which use automated tools to predict and deliberate.

The NSWCCL largely agrees with this definition of ADM, including the listed examples. However, we note the term "automated systems" is defined with reference to a range of technologies, which does not amount to a definitive defined term. In the NSWCCL's view, this is a critical omission, as the scope of application and purpose of the legislation may turn on how "automated systems" is defined.

The NSWCCL submits that the definition of "ADM" and "automated systems" will need to be compared with the definition of "AI systems" to ensure alignment, and that there are no material gaps or overlaps between the definitions which lead to uncertainty in how they are applied.

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?

(a) Risks

The proliferation of AI poses significant risks to Australians' civil rights, and our existing patchwork of regulations inadequately addresses them. These include, significantly:

1. Opaque decision-making processes that lack transparency and explainability;

2. Biased decision-making leading to unfair outcomes;

3. Potential for use in ways harmful for democratic discourse (such as generating misinformation to confuse citizens); and

[8] OECD Recommendation of the Council on Artificial Intelligence, adopted on 22 May 2019 (OECD Legal/0449), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

4. Use in ways that violate rights to privacy and civil liberties (eg, trained on scraped data involving sensitive personal information, or use in surveillance programs).

(b) The NSWCCL's proposed regulatory approach

(i) A "Jigzaw" regulatory approach: A risk based approach to AI regulation that utilizes a combination of existing and tailored regulatory tools is required

As is evidenced by the successive inquiries into AI (of which this review is the latest, welcome, iteration), Australia's historic approach to the regulation of AI has been fragmented. However, the NSWCCL reiterates its view that no single piece of legislation can adequately protect individuals from the existing and emerging risks of adopting AI.[9] Instead, a well coordinated combination of regulatory tools and resources to regulate AI and mitigate risks in a responsible manner is required. The NSWCCL considers this can be facilitated through a coordinated "jigsaw" regulatory approach, comprising of:

1. Reforms to existing laws – primarily privacy and data protection laws, and consumer laws, to bring alignment in approach to accounting for the risks or negative consequences of AI. In particular, the ongoing Privacy Act review should account for the privacy risks posed by the use of AI;[10] and

2. Bespoke AI legislation that adopts a risk-based approach, with clear and proportionate obligations on entities that develop, deploy or use AI, and safeguards to protect the rights of individuals. The legislation must ensure a high level of protection for privacy, measures to be put in place to prevent discriminative design and use of AI and a right to due process where AI is used in decision-making.

(ii) Creation of an AI Safety Commissioner

For such an approach to be effective, however, the NSWCCL believes that a separate statutory office for an AI Safety Commissioner is necessary to coordinate regulatory responses (monitoring and enforcement) across Australia. This builds on previous recommendations of the Australian Human Rights Council (**AHRC**) in its 2021 *Human Rights and Technology* report.[11] Although the existing office of the OAIC will have some overlap with a new AI regulator, the NSWCCL submits that the OAIC is already under-resourced and overburdened in the handling of privacy and freedom of information claims.

NSWCCL submits that a standalone AI Safety Commissioner warrants consideration having regard to the following:

- AI and ADM are emerging technologies with a wide suite of applications and potential risks and harms including for consumers, government and more broadly society.

- Effective regulatory oversight is likely to require fundamentally different considerations and specialised skillsets to adequately monitor and regulate to ensure consumers and society are safeguarded from emerging threats and risks. Regulatory oversight specific to AI and ADM will therefore require appropriate sanctions and enforcement powers.

- A stand-alone, specialised AI Safety Commissioner would be able to develop technical and regulatory capacity that will not only be able to provide an intervene in relation to AI / ADM specific legislation, but also assist other regulatory bodies in regulating AI and ADM related issues that are regulated under other existing legislative regimes.

[9] NSWCCL Submission to ADM and AI Regulation Issues Paper, 6-7.
[10] See, NSWCCL Submission to Privacy Act Review.
[11] AHRC, *Human Rights and Technology* (Final Report, 2021) 127.

- An AI Safety Commissioner may also increase public trust in the use of AI and ADM, as there would be dedicated / expert oversight of government and private applications of these technologies, and a specialised body to which the general public can bring complaints. As illustrated by Robodebt, there are few, if any, accessible avenues of recourse available for individuals adversely affected by ADM or AI.

The AI Safety Commissioner should have jurisdiction to oversee Commonwealth and State public agencies and private sector organisations. Most state government agencies are separately subject to their respective state regulators and state privacy and freedom of information legislation. Use of AI and ADM is relevant in both the public and private sector contexts on a state and federal level, and so a coordinated approach with state regulators is recommended.

In order to be effective, the NSWCCL submits that the AI Safety Commissioner must receive adequate resourcing, both in terms of funding and personnel. The Department's AI Action Plan includes a targeted $124.1 million investment over 2021-2022 to strengthen Australian leadership in developing and adopting responsible AI.[12] In the context of this phase of the AI Action Plan, it has placed its focus on supporting business adoption of AI. The NSWCCL submits that the responsible use and development of AI and ADM is dependent on directing some of that governmental support and funding towards the establishment of a separate AI Safety Commissioner, for the reasons outlined above. The adequate funding of an AI Safety Commissioner will allow it to develop its own capabilities side-by-side business and Government as these technologies and their range of applications continue to evolve. Commentators have noted that European regulators are inadequately funded to attract the necessary expertise,[13] demonstrating the critical importance of adequate funding.

(iii) Implementation of risk-based approach to AI regulation

The NSWCCL reiterates its support for a risk-based approach to regulation of AI, whereby AI practices are subject to graduated regulatory requirements depending on the level of risk involved with their use. This is discussed further in section 5 (below). In addition, disclosure requirements should apply to private and public sector uses of AI in their decision-making. This is discussed further in section 9(b) (below).

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

A strong regulatory response is essential for mitigating the significant risks associated with unregulated AI practices. However, the NSWCCL supports complimentary non-regulatory responses.

For example, the California Privacy Protection Agency (**CPPA**), established by *California Privacy Rights Act of 2020* (Proposition 24), performs an educational function for the public and provides technical assistance to the legislature with respect to privacy-related legislation as well.[14] Greater understanding of AI (including its associated risks) by creators and users would allow for more effective regulation. An AI Safety Commissioner could similarly promote public understanding of AI, as well as providing guidance on how AI developers and deployers could create AI ethically and in conformity with applicable regulations.

[12] Australia's Artificial Intelligence Action Plan', Department of Industry, Science, Energy and Resources, (Web Page, June 2021) https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan/direct-ai-2021-22-budget-measures-implementation-and-next-steps.

[13] Alex Engler, 'Key enforcement issues of the AI Act should lead EU trilogue debate,' *Brookings* (online article, 16 June 2023) https://www.brookings.edu/articles/key-enforcement-issues-of-the-ai-act-should-lead-eu-trilogue-debate/.

[14] See further, NSWCCL Submission to DPM&C, ADM and AI Regulation Issues Paper, 15.

The NSWCCL also submits its support for industry-led bodies that could promote ethical and regulatory-compliance development and deployment of AI. This could be useful to address specific issues associated with AI in particular sectors. For example, the 'Veritas Initiative' in Singapore has aimed to support the implementation of fairness, ethics, accountability and transparency (FEAT) principles developed by the Monetary Authority of Singapore in the use of AI by the financial sector.[15] Such initiatives could promote "buy in" from industry, and provide a useful forum for the AI Safety Commissioner to raise or identify emerging concerns.[16]

The NSWCCL believes, however, that such bodies should remain distinct from regulators. Some commentators have noted that, throughout the drafting of the European Union's proposed *Artificial Intelligence Act* (**AI Act**), AI developers have effectively lobbied for a softer regulatory response.[17] While developers and deployers will play an important role in the formation of AI regulatory policy in Australia, independent oversight is required to ensure the objectives of transparency, accountability and fairness are achieved.

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.

Please see NSWCCL's submission above in relation to Q2. Further, the NSWCCL submits that an AI Safety Commission could effectively facilitate coordination of AI governance across government agencies whereby it:

- has a statutory duty to report findings / recommendations to Government and other regulators (including Office of the Australian Information Commissioner (**OAIC**) and Australian Competition and Consumer Commission (**ACCC**));
- can conduct inquiries at the request of the Treasurer; and
- refers matters for enforcement to the ACCC, Commonwealth Director of Public Prosecutions and OAIC (as appropriate).

NSWCCL suggests that the goals for the AI Safety Commissioner as a coordination mechanism should be consistent with a risk based approach to AI regulation, namely to:

- ensure accountability and transparency;
- ensure vulnerable groups are afforded extra protections; and
- encourage uptake of responsible AI / ADM applications by both private and public sectors.

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?

The NSWCCL supports adoption of a risk-based approach to AI that is informed by international best-practice.

In particular, regard should be given to the EU's proposed AI Act and Canada's proposed *Artificial Intelligence and Data Act* (**AIDA**), both of which use risk-based models for AI regulation. Of these, the NSWCCL submits the AI Act to be the more comprehensive and sophisticated, and therefore we discuss

[15] Ibid, 11.
[16] See generally, Ian Ayres and John Braithwaite, *Responsive Regulation* (Oxford University Press, 1992) 101-157.
[17] See, Jess Weatherbed, 'The EU still needs to get its AI Act together,' *The Verge* (online article, 29 June 2023) https://www.theverge.com/2023/6/29/23777239/eu-ai-act-artificial-intelligence-regulations-europe; Billy Perrigo, 'Exclusive: OpenAI Lobbied the EU to Water Down AI Regulation,' *Time* (online article, 20 June 2023) https://time.com/6288245/openai-eu-lobbying-ai-act/.

it in some detail through this section. The AI Act is currently undergoing a lengthy, iterative drafting process. In May 2023, the Internal Market Committee and the Civil Liberties Committee of the European Parliament adopted a draft negotiating mandate that amends the draft proposed by the European Commission (the **Revised AI Act Draft**).[18]

There are several aspects of the Revised AI Act Draft that the NSWCCL believes bear consideration:

(a) A risk-based system of regulation

The AI Act imposes differing levels of restrictions and regulations based on the level of risk associated with the AI used, adapting a risk-categorisation system from EU product safety law.[19] AI practices involving an "unacceptable level of risk", listed in Article 5 of the Revised AI Act Draft, are prohibited.[20] AI systems that pose a high risk to health and safety to fundamental human rights ("high-risk AI systems") are subject to mandatory regulations.[21] These include requirements that they:

1. Implement adequate risk assessment and mitigation systems;
2. Use high quality datasets in training their systems to minimise risks and discriminatory outcomes;
3. Maintain a log of activity to ensure traceability of results;
4. Complete and maintain detailed documentation about the system for authorities to assess its compliance;
5. Provide clear operation guidances to users;
6. Have an appropriate level of human oversight measures to minimise risks; and
7. Maintain a high level of robustness, security and accuracy.

The Revised AI Act Draft also contemplates that the European Commission would create specific standards for high-risk AI which, if met, would allow developers to assume they have discharged their obligations under the Act.[22] Other AI is subject to less onerous, voluntary regulatory standards.

There are, however, limitations to the AI Act that demonstrate the difficulties inherent to a risk-based system of regulation. First, as noted by Nathalie Smuha et al[23] and Michael Veale and Frederik Zuiderveen Borgesius,[24] AI providers are given significant scope to self-judge the risks associated with their AI systems. Under Article 9 of the Revised AI Act Draft, providers of high-risk AI systems are required to implement and maintain a risk management systems. However, providers are also left to determine what residual risks associated with their systems are "reasonably judged to be acceptable."[25] The NSWCCL would not support a similar level of discretion for providers of high-risk AI systems under Australian regulations. At the very least, if AI providers were to be afforded such discretion they should

---

[18] Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, European Parliament, *Draft Compromise Amendments on the Draft Report: Proposal for a regulation of the European Parliament and of the Council on harmonised rules on AI (AI Act) and amending certain Union Legislative Acts* (version 1.1, 16 May 2023) https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf. See also, 'AI Act: a step closer to the first rules on Artificial Intelligence,' *European Parliament News* (Press Release, 11 May 2023) https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

[19] Michael Veale and Frederik Zuiderveen Borgesius, 'Demistifying the Draft EU Artificial Intelligence Act,' *Computer Law Review International* no. 4 (2021) 97, 102 [33].

[20] Revised Act Draft, art 5.

[21] Ibid, Title III.

[22] Ibid, art 40.

[23] Nathalie Smuha, Emma Ahmed-Rengersb Adam Harkens, Wenlong Li, James MacLaren, Riccardo Pisellif and Karen Yeung, 'How the EU can achieve legally trustworthy AI,' (Report, LEADS Lab@University of Birmingham, 5 August 2021) https://deliverypdf.ssrn.com/delivery.php?ID=158006120027098087072123116123096023022073004041071075072106111101110077002122079099004009106006041043008021112085090012119120027034008006040082030022031012116084023004006016106082005101119082003090003000087071108119008075127081094109080030080018077097&EXT=pdf&INDEX=TRUE

[24] Michael Veale and Frederik Zuiderveen Borgesius, 'Demistifying the Draft EU Artificial Intelligence Act,' *Computer Law Review International* no. 4 (2021) 97.

[25] Revised AI Act Draft, art 9(4).

be (i) required to consult with affected persons, or (ii) justify to regulators and users why such levels are acceptable.

Secondly, providers of high-risk AI are largely left to self-assess whether they have met the applicable standards. The AI Act is entwined with the EU's *New Legislative Framework*[26] which creates a common EU approach to regulation of certain consumer and medical products. Under that framework, manufacturers self-assess whether their products meet standards produced by prescribed organisations. If their products meet those standards (which are created by prescribed standards bodies), they may presume they have conformed with the essential requirements of the AI Act.[27] All AI providers, except providers of high-risk AI involving biometric information, will be able to self-assess compliance.[28]

The NSWCCL would, in principle, support the creation of more specific standards developed by the AI Safety Commissioner that high-risk AI must meet before release on the Australian market. This would allow for greater certainty and consistency for developers and deployers, as well as promote public trust in AI use.[29] For these to be effective, adequate funding of the Commissioner would be vital to attract experts in AI to develop and test to these standards.[30] The NSWCCL would, however, object to reliance on self-testing by developers. At minimum, randomised independent testing of AI should be required to ensure general compliance with standards.

Despite these drawbacks, the AI Act remains the most comprehensive and sophisticated international model of risk-based AI regulation to draw guidance from. The NSWCCL supports a risk-based approach as it balances regulatory burdens with regulatory risk, and directs finite regulator resources to high-risk areas. For such a system to work, however, the NSWCCL believes strong regulatory oversight (not reliance on self-assessment and self-judging of "acceptable risk") would be necessary, alongside adequate funding of an AI Safety Commissioner.

(b) Prohibition of specific forms of AI

The NSWCCL supports a flexible yet consumer welfare centric approach to defining which kinds of AI should be prohibited under a risk-based approach. An Australian approach should consider the list of prohibited AI forms as described in the Revised AI Act Draft (extracted and further discussed in section 10, below).

(c) Distinct obligations for providers of foundation models

The Revised AI Act Draft creates distinct obligations for providers of foundation models. Foundation models are machine learning models trained on extremely large datasets that can be used for various downstream uses (for example ChatGPT is a foundation model that is used as the basis for a number of generative text applications). Under the Revised AI Act Draft, foundation model providers must mitigate "*reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law*" throughout its development.[31] They must also register their models to an EU database, and must disclose whether any copyrighted data was used to train them.[32] Given the wide impact foundation models can have, the NSWCCL supports more onerous transparency and harm-mitigation obligations for their developers.

---

[26] Made up of European Parliament Regulation (EC) 765/2008, European Parliament and European Council Decision 768/2008 and European Parliament and European Council Regulation (EU) 2019/1020.
[27] Revised AI Act Draft, art 40.
[28] Ibid, arts 43(1), 63(5).
[29] By way of background, there are already a number of standards for manufacturers of various kinds of products to meet in Australia. Electrical goods cannot be sold or imported to Australia unless they meet standards set under the Electrical Equipment Safety System: see, Intergovernmental Agreement for the Electrical Equipment Safety System (2019). International standards bodies have began to develop standards applicable to some aspects of AI. For example, the International Organization for Standardization has developed ISO/IEC TR 24027:2021 (standard and specifies measurement techniques and methods to address bias-related vulnerabilities). Standards Australia has adopted this in SA TR ISO/IEC 24027:2022.
[30] European regulators are already beginning to struggle with this: see, Alex Engler, 'Key enforcement issues of the AI Act should lead EU trilogue debate,' *Brookings* (online article, 16 June 2023) https://www.brookings.edu/articles/key-enforcement-issues-of-the-ai-act-should-lead-eu-trilogue-debate/.
[31] Revised AI Act Draft, art 28b 2(a).
[32] Ibid, art 28b 2(g).

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

(a) Regulatory oversight

The NSWCCL supports the creation and adequate funding of an AI Safety Commission to oversee the use of AI by public and private organisations. Similar risks emerge in both contexts, demanding similar responses. Moreover, regulating the use of AI technology developed by private sector organisations and used by public agencies would create challenges if public/private sector use was regulated by different bodies.

(b) Regulatory requirements

The NSWCCL supports the same basic regulatory requirements, as outlined in section 5 (above), applying to both public and private sector uses of AI.

As discussed in greater detail in section 9 (below), both public and private sector organisations should also be subject to the same *minimum* requirements of fairness and transparency where AI is used in their decision-making. However, due to the democratic significance of government decision-making, the importance of maintaining the public's integrity in public institutions and agencies, and the ability of Government to impact vulnerable populations (eg. Robodebt), AI use by public sector organisations should be subject to additional, more onerous, transparency requirements (as explained at section 9 below).

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

In addition to the above, the NSWCCL supports basic educational programs for government agencies on responsible use of AI. Such programs should cover:

- A basic outline of how AI used by the agency operates;
- Potential risks associated with use of their AI programs; and
- Strategies the agency can take as a deployer to avoid or mitigate such harms.

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.

(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?

Transparency must be ensured at each stage of the AI lifecycle. In this respect, consideration should be given to the "Transparency by Design" framework (modelled after "Privacy by Design"), proposed by Felzmann and colleagues.[33] They propose nine principles, divided between the three key stages of AI: (i) design for AI systems, (ii) information on data processing and analysis, and (iii) accountability. These principles focus on tracking and explanation at each stage of the data being used, how that data is being processed, understanding the audience and non-technical stakeholders to whom the AI system will be addressed, the decision-making process for data processing and the justification, and being able to explain the limitations and associated risks of the AI system. Systems should be designed to be able to be audited and AI decision-making should be designed so the process of its decision-making can be traced.

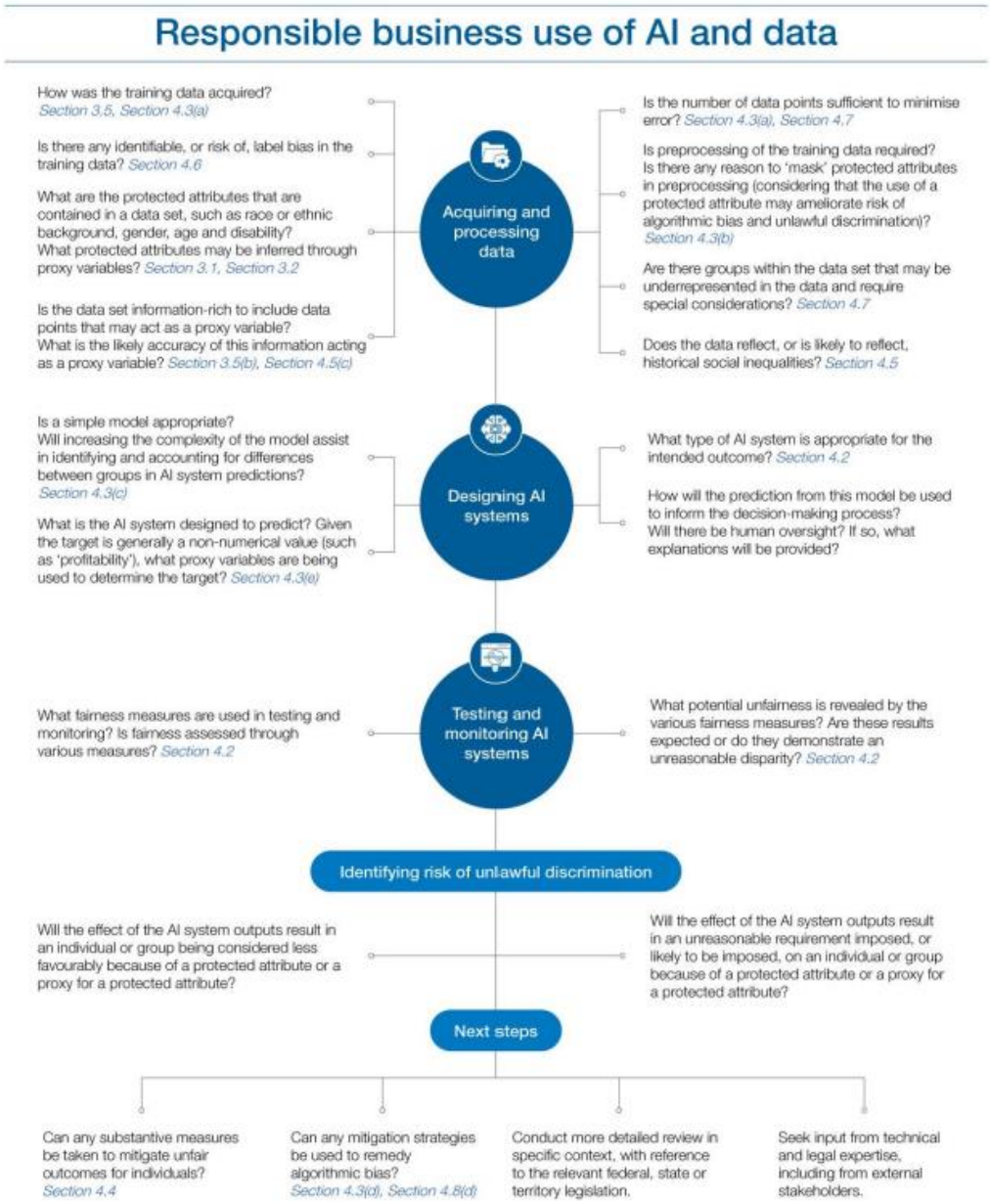
What Felzmann et al offer is a reflective tool that points out just how complex and multi-faceted transparency is in AI systems. They do not offer a concrete methodology, as transparency will look different and may evolve in the context of a particular AI technology. For example, Chris Reed distinguishes between *ex ante* transparency, where the decision-making process can be explained in advance of the AI being used, and *ex post* transparency, where the decision-making process can be discovered retrospectively.[34] Reed points out that AI technologies such as neural networks would struggle to achieve *ex ante* transparency, and the law must consider what kinds of transparency it mandates as this may also have a flow-on effect in hampering AI innovation and the use of particular technologies.

By way of an example, the AHRC highlights the importance of considerations for fairness, transparency and explainability through all stages of AI development. In a 2020 technical paper on algorithmic bias in AI decision-making, they provide a set of different questions for responsible developers to ask throughout the AI lifecycle (see figure 1, below). As the model demonstrates, responsible AI development must start at the training stage (ensuring training data is appropriately selected and cleaned) through to the deployment stage (where mitigation measures are considered).

[33] Heike Felzmann et al, 'Towards Transparency by Design for Artificial Intelligence', (2020) 26 Science and Engineering Ethics 3333, https://link.springer.com/article/10.1007/s11948-020-00276-4.

[34] Chris Reed, 'How should we regulate artificial intelligence?' in Sofia Olhede and Patrick Wolfe (eds) 'The growing ubiquity of algorithms in society: implications, impacts and innovations', Philosophical Transactions of the Royal Society, (2018, Royal Society) https://royalsocietypublishing.org/doi/full/10.1098/rsta.2017.0360.

Figure 1. The AHRC's responsible AI development model[35]



(b) Where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?

(i) The same basic standards of transparency should apply to private and public sector AI-facilitated decision-making

While much emphasis has been placed on the risks involved in the automation of government decision-making,[36] private sector organisations' use of AI can have equally profound effects on persons' lives. A decision by a bank to approve a home loan, a corporation to employ a person or an insurer set premiums for a person can have equally profound effects as government decisions. Where AI is used in these processes (which it increasingly is) minimum standards of fairness and explainability should be implemented. The NSWCCL therefore supports recommendations made by the Australian Human Rights

[35] Extracted from AHRC, *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias* (Technical paper, 2020) 55.
[36] Most significantly, through the massive harms to vulnerable social services users through the Robodebt Scheme: Royal Commission into the Robodebt Scheme (Report, 7 July 2023).

Commission (**AHRC**) in its 2021 *Human Rights and Technology Report*, that the following rules should apply to public and private sector decision-making using AI:

1. Individuals should always be notified of the use of AI in decisions affecting them, and the way in which it is used.

2. Use of "black box" or otherwise opaque AI should be prohibited.

3. Individuals should be given a practical means of seeking information from a natural person and appeal decisions made about them that involved an AI.[37]

The NSWCCL also supports clear disclaimers being provided to users wherever AI is deployed (regardless of AI risk level, the nature of its use or the sector deploying it).

(ii) Public sector organisations should be subject to additional transparency requirements

That being said, public agencies should be subject to more stringent transparency and accountability requirements than their private counterparts. This is because:

1. Democratic accountability demands government agencies be open and transparent to the public, and their decisions be fair and explainable;

2. AI deployment by government agencies inherently involves greater risk to human rights, especially where used in administrative decision-making with regards to citizens' rights or by law enforcement bodies;

3. When AI and algorithms are deployed on a wide scale applicable to large sections of the population, they can be subject to immutability and difficult to change, which in turn can make government agencies may be more unwilling and unable to take responsibility for unintended outcomes and consequences; and

4. Public agencies are not subject to the same profit-seeking incentives of private sector organisations; private sector developers have rights to keeping their technologies private as valuable intellectual property.

The NSWCCL supports a number of transparency and accountability measures that should apply to public sector AI use, such as the:

1. Creation of a database of AI used by government agencies (including Commonwealth, State and Local governments), to be maintained by the AI Safety Commissioner;

2. Publication of source codes for AI developed or used by government agencies along with the AI database;[38]

3. A simple, publicly accessible statement that explains (i) the kind of AI used by the agency, (ii) an explanation of how it is used, what kind of information is used in its application and (iii) the process to speak with a natural person;

4. A right for citizens to speak to a natural person rather than interfacing with an AI system when interacting with government agencies, or to seek review of an AI-facilitated decision (in addition to a prohibition on the use of AI in administrative decisions involving discretion, see further below); and

[37] Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) 12.
[38] See, Anna Huggins, 'Addressing Disconnection', *UNSW Law Journal* 44(3) (2021) 1048, 1066.

5. Development of guidance on how to responsibly use AI (including adequate testing mechanisms, education on the scope of responsibility of agencies using third-party-developed AI and how agencies can respond to errors occurring at large scale with their AI deployment).

The NSWCCL believes that measures for greater transparency must include measures that make government use of AI clear to persons without technical understanding of coding. For that reason, publication of source code itself would be insufficient to promote transparency and accountability for public sector AI use.[39]

In addition, the NSWCCL supports a systematic review of the use of AI and ADM systems in administrative decision-making. As the NSWCCL raised in its submission to the DPM&C ADM and AI Regulation Review, a developed response to the systemic issues associated with automated government decision-making is needed.[40] Non-binding policy guidance – such as the Commonwealth Ombudsman's 2020 guidance[41] or the Administrative Review Council's 2004 review[42] – has been insufficient. While many of the destructive uses of ADM systems have not involved the use of AI (notably, the Robodebt scheme) the increasing use of AI within government decision-making heighten the risks to citizens' rights and the erosion of trust in public institutions, agencies and democratic processes.

A key area where AI may impact government decision-making is the possibility for its use to provide judgements on questions involving discretion. As it stands, it is unclear whether administrative bodies may use ADM systems or AI in such ways.[43] The Administrative Review Council's 2004 report, argued that it was "not in accordance with the administrative law values of lawfulness and fairness because it could fetter their discretionary power,"[44] though this remains non-binding guidance.

The NSWCCL believes that the position in Australia should be clarified, with a prohibition on the use of AI or ADM systems in decisions involving discretion. AI systems are often "black boxes", meaning their reasoning is opaque even to their own developers.[45] This is contrary to the principles of fairness and explainability that should govern government decision-making.[46] The fact that generative AI systems can offer reasons for their decisions is cold comfort. As computer systems scholar Dr Matthew Hillier notes in a discussion of ChatGPT, it is "designed to produce the most plausible or probable, realistic reading language output relevant to the context of the prompt it has been given."[47] That is to say, a generative AI system may be able to make decisions and offer reasons, but the reasons offered will not necessarily reflect the actual process conducted in making its choice, and will rather provide a "plausible" reason for its output.

Finally, to assist the AI Safety Commissioner's work, departmental secretaries and agency chief executive officers should be subject to statutory duties to use their best endeavours to assist the Commissioner in any investigation into their agencies. It would be exceedingly difficult for the AI Safety Commissioner to inquire into proper use of AI by government agencies without this level of assistance. This adapts a recommendation made by the Royal Commission into the Robodebt Scheme, which would require secretaries and officers to support investigations by the Commonwealth Ombudsman.[48]

[39] Ibid, 1058 n 68, 1066.
[40] NSWCCL Submission to ADM and AI Regulation Issues Paper, 11-12.
[41] Commonwealth Ombudsman, *Automated Decision-Making: Better Practice Guide* (Report, 4 March 2020
[42] Administrative Review Council, *Automated Assistance in Administrative Decision Making* (Report to the Attorney General, 2004).
[43] Commonwealth Ombudsman, Automated Decision-Making: Better Practice Guide (Report, 4 March 2020) 9.
[44] Administrative Review Council, *Automated Assistance in Administrative Decision Making* (Report to the Attorney General, 2004) 15.
[45] Anna Huggins, 'Addressing Disconnection', *UNSW Law Journal* 44(3) (2021) 1048, 1065. See generally, Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, 2015).
[46] Huggins (above) 1065-6.
[47] Matthew Hillier, 'Why does ChatGPT generate fake references?' *Teche* (online publication, 20 February 2023) https://teche.mq.edu.au/2023/02/why-does-chatgpt-generate-fake-references/.
[48] Royal Commission into the Robodebt Scheme (Report, 7 July 2023) xix (Recommendation 21.1).

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?

Yes – the NSWCCL believes some AI applications pose an unacceptable risk of harm and should be banned entirely. The difficulty for policy makers is defining applications that should be prohibited. Given the pace of development and proliferation of AI, it is difficult to define in advance which AI applications pose an unacceptable risk of harm. Therefore, the NSWCCL supports an approach to prohibition where:

1. Certain high-risk AI applications are specifically identified and banned in legislation;

2. Legislation creates an objective test for AI that should be prohibited (such as AI posing "unacceptable risk of systemic, irreversible or perpetual harms to humans"); and

3. Legislation provides for delegated power to the Department Minister, on advice of the AI Safety Commissioner, to prohibit further high-risk AI that poses unacceptable risks of harm as they emerge.

With regard to (1), the NSWCCL broadly supports prohibition of the same list of AI technologies banned by the EU Revised AI Act Draft, including:

1. The use of subliminal techniques or exploitation of a person's age or ability in a way that causes physical or psychological harm;

2. "Real-time" remote biometric identification systems in publicly accessible spaces;

3. "Post" remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorisation;

4. Biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);

5. Predictive policing systems (based on profiling, location or past criminal behaviour);

6. Emotion recognition systems in law enforcement, border management, workplace, and educational institutions; and

7. Indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights and right to privacy).

There are, however, improvements that could be made to how the Revised AI Act Draft defines certain categories of prohibited AI. As has been noted by Veale and Borgesius in reference to banning high risk AI applications in legislation, there are difficulties in defining prohibited AI by reference to harm caused.[49] They argue that it is difficult to prohibit only those manipulative systems that cause harm, as the forms of manipulation AI systems use can be difficult to detect and operate through "underlying dynamics rather

[49] Michael Veale and Frederik Zuiderveen Borgesius, 'Demistifying the Draft EU Artificial Intelligence Act,' *Computer Law Review International* no. 4 (2021) 97, 99-100.

than one-off events".[50] In this regard, State coercive control offences could be considered as models for drafting harm-based definitions of prohibited AI. These offences are defined by reference to underlying dynamics or "course[s] of conduct",[51] rather than one-off instances of harm.

In addition, definitions that require intention on the part of the user or deployer (eg, if only subliminal techniques "designed" to cause physical or psychological harm were prohibited) will be difficult to enforce in practice. This is because it will often be difficult to identify developers' intention where large teams of developers have been involved in AI development, different teams of developers have worked on the AI (such as where developers have created a foundation model and a different set of developers have built a downstream application) or where AI is itself used to develop new AI applications. The NSWCCL submits that if "harm" is used to define prohibited AI applications, it should not involve an intention requirement.

As discussed in more detail in section 6 (above), the NSWCCL would also support prohibition of use of AI in administrative decisions which involve a level of discretion for the decision-maker.

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

The NSWCCL respectfully submits that the Department should not seek to increase public trust in AI deployment until it has more fully understood the risks and determined a responsible, and well considered, roadmap forward.

Significant risks are inherent to AI deployment: it has been used to operate bots to spread disinformation online, threatens large-scale replacement of jobs[52] and generate biased results.[53] While AI also offers opportunities to Australians, some level of distrust is justifiable. In this context, the NSWCCL argues that the only way in which government should seek to improve public trust in AI is by ensuring it is regulated effectively and forced to uphold the values of transparency, explainability and accountability (particularly when used by government agencies) in the ways suggested throughout this submission.

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

As already discussed, the NSWCCL supports a risk-based approach to AI regulation.

Such an approach, if implemented and managed effectively, allocates compliance burdens and finite regulatory resources according to risk of harm. Risk-based regulation of AI is more principally sound than regulation based on organisation size. The purpose of AI regulation should be to minimise harm to the public, and not to increase the compliance burden on developers and deployers unnecessarily. Organisations' size (whether measured by revenue or number of employees) is no proxy for potential harm of AI deployment. This is especially true for AI start-ups, which may have significant market impacts with small teams and initially no revenue, but significant impact on users.

[50] Ibid.
[51] *Crimes Act 1900* (NSW) s 54D.
[52] Committee for Economic Development of Australia, *Australia's Future Workforce?* (Report, June 2015) https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/researchcataloguedocuments/research%20and%20policy/pdf/26792-futureworkforce_june2015.pdf.
[53] Eirini Ntoutsi, Pavlos Fafalios, Ujwal Gadiraju, Vasileios Iosifidis, Wolfgang Nejdl, Maria-Esther Vidal, Salvatore Ruggieri et al. "Bias in data-driven artificial intelligence systems—An introductory survey," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 10(3) (2020): e1356.

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

There are some limitations to this approach. The compliance burden of a risk-based approach may be significant for smaller organisations, though (as stated above) this is outweighed by the risks to potential users as well as the benefit to large organisations which use only low-risk AI. In addition, the AI Safety Commissioner should play an important role in promoting understanding of new AI regulations by providing compliance guidance for small businesses.

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?

As discussed in sections (2) and (3) above, the NSWCCL believes that complimentary voluntary regulation should sit aside mandatory minimum requirements. As discussed in sections 6 and 9 (above), the same basic regulations should apply to public and private organisations, subject to some further requirements on public organisations.

The NSWCCL argues these should apply to developers and deployers, with tiered obligations based on risk. We refer to our discussion at section 9(a) (above) about the importance of considerations for transparency and fairness at all stages of AI development and deployment.

We trust this submission is of use to the Department and would be happy to participate in future discussions.

Yours sincerely,

Sarah Baker
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission: Anne Charlton
Email: anne.charlton@nswccl.org.au Mobile: 0400 433 743

NSW Council for Civil Liberties Inc.
PO Box A1386, Sydney South,
NSW 1235, Australia

e: office@nswccl.org.au
t: 02 8090 2952
www.nswccl.org.au

@nswccl
@nswccl

ANNEX 1

NSWCCL SUBMISSION

DEPARTMENT OF THE PRIME MINISTER AND CABINET

DIGITAL TECHNOLOGY TASKFORCE

POSITIONING AUSTRALIA AS A LEADER IN DIGITAL ECONOMY REGULATION – AUTOMATED DECISION MAKING AND AI REGULATION – ISSUES PAPER

20 May 2022

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

REVIEW OF AUTOMATED DECISION MAKING AND AI REGULATION

NSWCCL's response to Automated Decision Making and AI Regulation Issues Paper

1. OVERVIEW

The New South Wales Council of Civil Liberties (**NSWCCL**) thanks the Digital Technology Taskforce for the opportunity to make this submission in connection with the Issues Paper - Positioning Australia as a leader in digital economy regulation: Automated Decision Making and AI regulation.

Individuals in the digital information age that we live in today are increasingly becoming subject to scoring and classification performed by a range of increasingly sophisticated and ever improving digital technologies. As the sophistication of such technologies improves, the range of applications for such technologies is diversifying quickly. Indeed, automated decision making (**ADM**) and artificial intelligence (**AI**) have come to support, pre-empt and substitute human decisions in an increasingly diverse range of fields and industries, including online advertisement, medical diagnosis, credit lending, job applicant selection, government welfare decisions and even criminal justice. While the expanding application of these technologies is indicative of the efficiency and wide range of benefits they offer, designing a fit-for-purpose regulatory regime will necessarily ensure vulnerable Australians are adequately protected, and incorporate principles and legislative instruments that ensure transparency and accountability to safeguard individual autonomy and protect fundamental civil liberties.

NSWCCL submits that law reform is required to provide stronger, clearer and more targeted human rights protections regarding the development and use of AI and **ADM**. As AI and ADM are currently regulated within a broader system of regulation, NSWCCL submits that existing laws – particularly privacy, data protection, and consumer laws – should be reformed with an added focus on strengthening individual protections against the risks and negative consequences of AI and ADM. Furthermore, as AI and ADM pose specific risks for which there are currently legislative gaps, NSWCCL also recommends the implementation of legislation that is specific to mitigate risks to individuals and consumers posed by AI and ADM. NSWCCL considers that any improvements or implementations of legislation should prioritise transparency, explainability, accountability, responsibility / oversight and enforcement mechanisms (including sanctions), to avoid harms caused through bias, discrimination, and impingement upon individual rights.

2. PROTECTION OF VULNERABLE AUSTRALIANS IS CRITICAL

The NSWCCL considers it vitally important that AI and ADM do not adversely impact populations of Australians that are already vulnerable and at risk. For instance, there is public concern that AI, and indeed ADM, disproportionately causes harm to vulnerable and marginalised communities and there have been several instances where AI has harmed particular groups.[1] The Centrelink Robodebt incident, which ultimately resulted in a number of vulnerable Australians self-harming,[2] is a textbook example of the disproportionate harm AI and ADM can inflect on vulnerable Australians.

It is therefore important for governments to consider and respond to the potential for AI and ADM to adversely impact vulnerable populations of Australians, particularly given the emerging trend of various state and Commonwealth governments making greater use of automation of decision-making.[3] Other developments of AI and ADM have included:

- The Commonwealth government has adopted a digital transformation strategy that aims to use automated systems to eliminate manual processing and case management, reducing the need for bespoke systems.
- The NSW government stated that 'it will start to 'test AI/cognitive/machine learning for service improvement' and implement 'full automation where appropriate'.

[1] See, eg, Australian Human Rights Commission, 'Human Rights and Technology', Final Report (2021) 45, 59, 107 100-1.

[2] See, Senate Standing Committtee on Community Affairs, Commonwealth Parliament, 'Accountability and justice: Why we need a Royal Commission into Robodebt', Final Report (May 2022) at 14, [2.24].

[3] Yee-Fui Ng, 'Institutional Adaptation and the Administrative State' (2021) 44(3) Melbourne University Law Review 889, 923-924 <https://law.unimelb.edu.au/_data/assets/pdf_file/0008/3898601/04-Ng-889.pdf>.

The 'Centrelink Robodebt' incident exemplifies the difficulty in regulating the design, development, and operation of AI, and of seeking redress and accountability when AI operates detrimentally or without a proper legal basis. Robodebt was the automated debt recovery program introduced by the Australian federal government in 2016 to ensure that Centrelink recipients were not under-reporting their income and, as a result, receiving more welfare payments than they were entitled to.

Robodebt operated by calculating a social security recipient's income on a fortnightly basis by taking annual income data from the Australian Taxation Office (**ATO**) and averaging it across a fortnight, and then finding the difference between (i) the amount of welfare that the social security recipient actually received based upon their *reported* fortnightly income in the relevant year, and (ii) the amount of welfare the social security recipient would have been entitled to receive each fortnight based upon income figure taken from the ATO.[4] This calculation and averaging process played a key role in over $720 million being erroneously taken from Centrelink recipients. Despite investigations by the Commonwealth Ombudsman and Senate committee inquiries, a class action suit had to be filed before the Government agreed to repay and recompense wrongly claimed debts.

In approving settlement of the class action brought in relation to the Robodebt incident, the Federal Court of Australia found that the Government had no legal basis on which to assert that those individuals owed debts to the Commonwealth – income averaging from ATO data did not provide that legal basis.[5] In such circumstances, over-reliance on AI can lead to shortcuts that end up violating individual legal rights in ways that would not have occurred had the same process been handled manually. More broadly, what the Robodebt incident has exposed is that there is a fundamental a gap in oversight and the existing regulatory framework in relation to the the use and impact of AI.

The increasing uptake in Australia and globally of automation in welfare programmes highlights just how risky and threatening AI and ADM can be for socially and economically vulnerable groups. As Yee-Fui Ng argues, it points towards the need for both individual redress – which was difficult, if not near impossible, to seek on an individual basis in the wake of Robodebt miscalculations – and independent scrutiny, such as regulator oversight, over governmental programmes.[6] The risk of removing human oversight entirely and placing our trust in AI systems is that AI systems can still be badly designed and operated due to human error, and to implement them on such a huge scale – such as in the context of the welfare state – risks an automated governmental response that it is too difficult to unwind and re-implement it. NSWCCL submits, therefore, that there must be avenues of redress and human scrutiny of AI systems with a view to protecting vulnerable populations and those who may be adversely affected by the outcome of AI systems, particularly when it comes to high-risk situations such as welfare, migration, employment, law enforcement, critical infrastructure, education, and other such circumstances that may limit access to justice.

3. ARTIFICIAL INTELLIGENCE

3. Introduction

While safe and effectively regulated AI has enormous potential to facilitate socially and environmentally beneficial outcomes, AI that is not responsibly designed and subject to sufficient oversight, review and (where appropriate) intervention poses a real and profound threat to human rights. More broadly, in the absence of a carefully designed regulatory regime, AI has the potential to reduce people to data points that are exploited for commercial and political gain without recourse. NSWCCL recommends law reform is required to develop a regulatory regime that provides stronger, clearer and more targeted human rights protections regarding the development and use of AI and ADM.

Any amendments to existing legislative regimes or new laws must consider impacts to human rights and ensure there are adequate safeguards, such as transparency and accountability measures, rights for review, appropriate (and well-resourced) regulator oversight and accessible and affordable enforcement measure (with sanctions). NSWCCL endorses a human rights approach to AI and believes that any approach to AI must include both an effective legal

[4] Second Further Amended Statement of Claim, *Katherine Prygodicz & Ors v Commonwealth of Australia*, VID1252/2019, Federal Court of Australia, <https://www.robodebtclassaction.com.au/media/1289/200914-second-further-amended-statement-of-claim-2fasoc-stamped.pdf>, [6].

[5] *Prygodicz v Commonwealth (No 2)* [2021] FCA 634, [59].

[6] Ng (above n 3),924.

regime, and "human rights by design" whereby human rights standards are embedded into the design, development and deployment of new technologies.[7] Law reform must work in tandem with co- and self-regulation that targets the design and development stage to avoid human rights issues occurring in the first place.

A proportionate risk-based approach will ensure that individuals are protected, particularly against high-risk AI systems that pose risks to human rights or exploit vulnerabilities of specific groups, while allowing AI systems to be safely used to support socially and environmentally beneficial outcomes.

3. Regulatory uncertainty and complexity

The Issues Paper notes concerns surrounding the complexity of the regulatory environment and the fact that there are multiple overlapping regulatory frameworks, including privacy law, anti-discrimination law, consumer law, and administrative law. Some of these frameworks are also not technology-neutral, creating further friction as technology develops and outpaces the purpose of existing regulation. To address this emerging legal uncertainty, and as prefaced above, NSWCCL submits that law reform is required.

As a starting point, NSWCCL submits there is also value in government conducting an exercise whereby the potential risks and harms that AI (and indeed ADM) poses are identified. This will facilitate an appropriate gap analysis with respect to the adequacy of existing laws, while identifying where new targeted laws are required.

Outlined below, we have sought to highlight where amendments to existing laws are likely required and where new specific legislation is likely warranted.

Amending Existing Laws

NSWCCL submits that existing laws – particularly privacy, data protection, and consumer laws – should be reformed and updated with an added focus on strengthening individual protections against the risks and negative consequences of AI. NSWCCL supports amending such legislation using a principles-based approach in order for the regulatory framework to be technology-neutral, ensuring the achievement of certain outcomes even as technology advances beyond the time the legislation was put in place.

This is in line with the Australian Human Rights Commission (**AHRC**), who stated in their 2021 Report that an outcome-based framework for regulation for AI should generally be promoted.[8] Rather than regulating particular technologies, regulation should focus on outcomes, for example a law could require decisions to be procedurally fair and consider certain matters rather than defining precisely how a decision maker must afford procedural fairness. Exceptions, however, should exist for when AI poses a significant risk to human rights. In this situation, direct regulation may be needed.

Part of this involves amending legislation to ensure legal entitlements already in existence continue to apply when AI or automation is used where they have not traditionally been used or are not provided for in law. For example, the AHRC states the *Acts Interpretation Act 1901* (Cth) should be amended to avoid any doubt that, when AI or automation is used in the decision-making process of an administrative decision, there is a legal entitlement to reasons for a decision. Any amendments should emphasise the impact on individuals rather than the technology used. NSWCCL supports this proposal, and in particular the need to amend legislation with an emphasis on the impacts on individuals and their rights, regardless of what technology is or is not used.

It has been countered that the concept of technology neutrality may not be as effective in practice because the effect of new technologies on existing legislative frameworks may be inconceivable.[9] NSWCCL, however, submits that a focus on principles and outcomes, with a view to ensuring equality, non-discrimination, freedom of expression, and procedural rights, is the best position where we are unable to know future technologies' impacts with certainty. Further, at the point where we know such impacts, it is likely that the government will hasten to amend the relevant regulatory frameworks.

---

[7] AHRC, 'Human Rights and Technology' (above, n 1).

[8] Ibid, p. 49.

[9] Australian Law Reform Commission, 'Should the Privacy Act be technology neutral? (Web Page, 16 August 2010), https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/10-accommodating-developing-technology-in-a-regulatory-framework/should-the-privacy-act-be-technology-neutral/

In the UK, there is a public sector equality duty that requires public authorities in the exercise of their functions to have regard to the elimination of discrimination, harassment, victimisation and any conduct prohibited under the UK Equality Act 2010, and advance equality of opportunity between those who share a protected characteristic and those who do not.[10] In *R v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, a claim was brought against the South Wales Police for using live facial recognition technology on multiple grounds, including non-compliance with the public sector equality duty. The Court of Appeal found that the South Wales Police had failed to do all that it could reasonably do to fulfil the duty in respect of its use of live automated facial recognition, including failing to establish whether the technology might be biased. In the Australian context, anti-discrimination laws are based on individual rights, rather than duties, so there is currently less legal protection as compared with the UK Equality Act 2010. This suggests there may be a need to build equality obligations into privacy or AI specific laws.

Furthermore, and drawing upon the UK experience, positive duties may also have a place in Australia. Such a strategy would open up enforcement actions and remedies to those who suffer specific ADM induced harms but fall outside the narrow scope of existing discrimination law. Moreover, the introduction of positive duties may encourage consideration of the important prior question of whether algorithms should be deployed in the first place, embedding equality considerations into the planning and design stage, rather than merely prompting deliberation about after-the-fact accountability for algorithmic discrimination. Indeed, NSWCCL suggests that in circumstances where there is a serious risk of harm or significant intrusion on individual rights, that a regulatory mechanism that requires alternatives to AI to be considered in the first instance may be appropriate.

- **Specific Legislation**

While there are multiple overlapping regulatory frameworks, there is no legislation that provides for AI specifically. This means that there are gaps particular to the operation and oversight of AI technologies. NSWCCL submits that Australia should put in place bespoke AI legislation with clear and proportionate obligations on entities that use AI, and safeguards to protect individual rights. NSWCCL considers that a technology-neutral, process-based definition of AI and the ecosystem in which it operates should be adopted in Australia.

While the NSWCCL generally supports a technology-neutral approach to law making in this area,] some uses of AI and specific articulations of the technologies raise such a significant and immediate risk to human rights that direct regulation may be required in these high-risk areas. The AHRC in its 2021 report suggested that specific laws may be required to address the use of AI in areas such as refugee status determinations, autonomous weapons, facial recognition, and biometric surveillance technology in contexts such as policing.[11]

In particular, where human rights are at urgent risk of infringement due to an AI technology, NSWCCL supports specific regulation to address those risks where the broad principles upheld by more general legislation are insufficient to protect against those human rights harms.

In Australia, there is no legal definition of AI and there are presently no statutes or regulations dealing specifically with AI. Rather, Australia's approach to regulating AI has, to date, comprised a soft law, principles-based approach through tools such as non-binding guidelines. For example:

- The Department of Industry, Science, Energy and Resources has set out eight AI Ethics Principles as part of a broader framework designed to ensure that AI is safe, secure, and reliable.[12] These principles are intended to act as voluntary guidelines.

- Certain components of other regulatory frameworks affect the use and adoption of AI – such as privacy law, anti-discrimination law, consumer law, and administrative law. However, none of these are AI-specific, and even where they provide protections that NSWCCL is in support of, they do not provide specific obligations regarding the use of AI, or protection from AI-related harms.

[10] Available online: https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf

[11] AHRC, 'Human Rights and Technology' (above, n 1) 49.

[12] Available online: https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles)

NSWCCL submits, therefore, that separate regulation in relation to AI may be required to regulate the fair adoption, use, and effect of AI by commercial and government entities. NSWCCL considers that a two-pronged approach to regulating AI in Australia is appropriate, consisting of:

1. Reforms to existing laws – primarily privacy and data protection laws, and consumer laws, to account for the risks or negative consequences of AI. In particular, the ongoing Privacy Act review should account for the privacy risks posed by the use of AI.

2. Bespoke AI legislation that adopts a risk-based approach, with clear and proportionate obligations on entities that use AI, and safeguards to protect the rights of individuals. The legislation must ensure a high level of protection for privacy, ensure equality and non-discrimination and prevent a chilling effect on freedom of expression. It must also protect the right to an effective remedy and to a fair trial, right of defence and the presumption of innocence.

Finally, NSWCCL considers that the privacy implications of the use of AI should be contemplated in the Privacy Act review, and any AI-specific regulation should be consistent with existing privacy obligations. This is particularly so where AI systems use personal data – this is an issue especially where the data used is inaccurate, as was seen in the Centrelink Robodebt incident described in above. This makes it even more important that notification when personal information is being used must occur.

3. Transparency, explainability, and bias

While safe and regulated AI has enormous potential to facilitate socially and environmentally beneficial outcomes, AI that is not responsibly designed and subject to sufficient oversight, review and intervention poses a real and profound threat to human rights. In particular, the deployment of AI can allow mass surveillance and unfair or discriminatory exercises of power, both public and private, due to the issues it raises in relation to bias, transparency, accountability, and explainability.

Bias

One principal issue that has been often recognised with regard to the issues associated with the government application of AI is that of bias.

- Perry and Campbell have noted how AI and machine learning risks create an "implicit assumption" that the decisions made by machines are inherently more superior and trustworthy than a decision coming from a human.[13] However, machines and AI may suffer some degree of bias due to the design process and the data used to train the system.

- The data on which AI systems are trained may reflect various forms of conscious and unconscious biases. This can perpetuate stereotypes and discrimination. For example, predictive policing uses deliberate modelling to push historic data into the future and attempt to forecast criminal activity. For crimes such as burglary, predictive models can be created based on the geographic area in which future burglaries are likely to occur.

- While most software mainly has a geographic focus, some identify at-risk individuals by creating profiles generated from historical data. This exploits historical biases in data and is likely to target those from a particular race, social class, gender, or age group. While this is a fairly obvious example, there are other situations in which those who train the AI systems may not realise at the start that there are particular patterns or biases in the data that they choose. As such, it is crucial to be able to access and understand the data that was used to train the system.

Transparency, Accountability and Explainability

Regarding transparency, accountability and explainability, it is unlikely that the general public will have any substantial knowledge on how the government is using AI and how the data gathered from AI and machine learning

[13] Hon. Justice Melissa Perry and Sonya Campbell, 'AI and Automated Decision-Making: Are You Just Another Number?' (Paper presented at *Kerr's Vision Splendid for Administrative Law: Still Fit For Purpose?*, online, 21 October 2021) 2.

is being used. Additionally, the complexity associated with AI makes it difficult to apply appropriate standards to judge an automated decision due to the following:

- The lack of explainability makes it difficult to provide adequate transparency and accountability. AI and machine learning are complex systems – this means that few individuals possess the requisite understanding and knowledge to comprehend how and why these systems behave in the way that they do. The mechanisms by which AI systems are created and trained often create a "black box", whereby the designers of an AI system are unable to explain how or why a particular output was produced. For example, MIT and Harvard scientists have found that an AI programme trained to read X-rays and CT scans could predict a person's race with 90% accuracy – and yet, the scientists who conducted the study could not explain how the AI programme was doing the prediction.[14] Designers may themselves have blind spots and may not realise the limitations of the data they use to train an AI system. As a result, explainability within AI should be encouraged, as otherwise it will be difficult to provide any basis for accountability. It is important to note that the kinds of transparency which are achievable vary between types of AI.

- Additionally, parties may not be aware that AI or machine learning was employed in a decision that had an impact on them. Intentional secrecy compounds this issue further. Data, algorithms, and the resulting AI systems are often treated as state or trade secrets or protected by privacy or data protection laws and are thus unreviewable to some extent.

- Courts may even find that the assessments and predictions given by AI are in line with due process. *State v. Loomis* 881 N.W.2d 749 (Wis. 2016) concerned an algorithmic risk assessment called COMPAS was used in sentencing Eric Loomis. COMPAS assessments use an interview with the offender and information from the offender's criminal history to estimate the risk of recidivism. The algorithm that undertakes the assessment is a trade secret, and only the estimates are reported to the court. The trial court referred to the COMPAS assessment in its sentencing determination and sentenced Loomis to six years of imprisonment and five years of extended supervision. Loomis filed for post-conviction relief, arguing that allowing the trial court to rely on the COMPAS assessment violated his due process rights. The Wisconsin Supreme Court (**WSC**) held that the use of an algorithmic risk assessment in sentencing did not violate Loomis' due process rights even though the methodology was not disclosed to the court or Loomis. The WSC introduced a procedural safeguard by requiring "written advisements" to be provided to alert judges to the dangers of these assessments, but judges are still likely to be influenced by the estimates provided by such assessments.

Methods for Improved Transparency for ADM and AI

Transparency is hampered in the context of ADM and AI in part due to the full basis for algorithmic decisions rarely being available to affected individuals. This is because the algorithm and inputs may be secret, the implementation may be secret, or the process may not be precisely described.[15] Anna Huggins has suggested that one way in which governments could better adhere to issues associated with transparency is to be required to make the source code of automated systems publicly available. [16] However, various commentators have suggested that transparent source code may still be insufficient at achieving algorithmic accountability particularly relating to individual decisions. This, as a result, necessitates additional safety measures. Since an individual can only challenge a particular decision or express their view if they understand how the decision was made and on what basis, notification to the affected individual, explanation of the process and a right to access information relating to the decision-making process are essential (see further discussion in section 2.3).

But even where processes are transparent in the sense of information being available, transparency requires more than this in each part of the AI lifecycle. Felzmann et al have put forward the concept of 'Transparency by Design', modelled after 'Privacy by Design', to serve as practical guidance in AI systems beyond calling for informational

[14] Hiawatha Bray, 'MIT, Harvard scientists find AI can recognize race from X-rays – and nobody knows how' (Online, 15 May 2022) <https://www.bostonglobe.com/2022/05/13/business/mit-harvard-scientists-find-ai-can-recognize-race-x-rays-nobody-knows-how/>.

[15] Dominique Hogan-Doran SC, "Computer says 'no': automation, algorithms and artificial intelligence in Government decision-making" (2017) 13 *The Judicial Review* 1, 2.

[16] Anna Huggins, 'Addressing disconnection: Automated decision-making, administrative law and regulatory reform', (2021) 44 *University of New South Wales Law Journal* 3, 1048-77.

availability.[17] They propose nine principles, divided between three key stages of AI: (i) design for AI systems, (ii) information on data processing and analysis, and (iii) accountability. These principles focus on tracking and explanation at each stage of the data being used, how that data is being processed, understanding the audience and non-technical stakeholders to whom the AI system will be addressed, the decision-making process for data processing and the justification, and being able to explain the limitations and associated risks of the AI system. Systems should be designed to be able to be audited and AI decision-making should be designed so the process of its decision-making can be traced.

What Felzmann et al offer is a reflective tool that points out just how complex and multi-faceted transparency is in AI systems. They do not offer a concrete methodology, as transparency will look different and may evolve in the context of a particular AI technology. For example, Chris Reed distinguishes between *ex ante* transparency, where the decision-making process can be explained in advance of the AI being used, and *ex post* transparency, where the decision-making process can be discovered retrospectively.[18] Reed points out that AI technologies such as neural networks would struggle to achieve *ex ante* transparency, and the law must consider what kinds of transparency it mandates as this may also have a flow-on effect in hampering AI innovation and the use of particular technologies.

NSWCCL submits that the legislation cannot simply require transparency, explainability, and accountability by requiring algorithms and source code to be published. While this is important, particularly in the context of trade secrecy, NSWCCL considers that improving transparency requires greater consideration of the role of transparency, explainability, and accountability at each stage of the AI lifecycle. While transparency must be balanced against competing considerations, such as AI innovation, NSWCCL submits that this cannot come at the cost of the key role that transparency, explainability, and accountability play in upholding individual human rights.] Accordingly, NSWCCL submits minimum standards for the development and utilisation of AI should be provided for.

3. Law makers should draw upon international developments and regulatory models

International regulatory developments provide useful models for Australian law makers to draw upon, particularly in relation to how legislation should approach the definition of AI. In this regard, the NSWCCL supports a legislative approach that focuses on outcomes and endorses the OECD approach with its focus on the process and output of AI systems, as this best appreciates the AI ecosystem and the impact – including the impact on human rights – of such an ecosystem.

OECD

In 2019, the OECD issued the OECD Recommendation on Artificial Intelligence. The Recommendation outlines five principles for the 'responsible stewardship of trustworthy AI': (i) inclusive growth, sustainable development and well-being; (ii) human-centred values and fairness; (iii) transparency and explainability; (iv) robustness, security and safety; and (v) accountability.

The OECD Recommendation understands AI through a number of terms:

- AI system lifecycle – comprising: (i) design, data, and models, (ii) verification and validation, (iii) deployment, and (iv) operation and monitoring;
- AI knowledge – the skills and resources (such as data, code, algorithms, models, research, governance, and best practices) required to understand and participate in the AI system lifecycle;
- AI actors – those who play an active role in the AI system lifecycle); and
- Stakeholders – all organisations and individuals involved in, or affected by, AI systems directly or indirectly.

[17] Heike Felzmann et al, 'Towards Transparency by Design for Artificial Intelligence', (2020) 26 *Science and Engineering Ethics* 3333, <https://link.springer.com/article/10.1007/s11948-020-00276-4>.

[18] Chris Reed, 'How should we regulate artificial intellegence?' in Sofia Olhede and Patrick Wolfe (eds) 'The growing ubiquity of algorithms in society: implications, impacts and innovations', *Philosophical Transactions of the Royal Society*, (2018, Royal Society). Available at https://royalsocietypublishing.org/doi/full/10.1098/rsta.2017.0360)

The OECD's distinction between AI actors and stakeholders is an incredibly useful way to understand the impact of AI, and its deliberate setting out of the AI system lifecycle makes it less likely that any shortcuts will be taken or blind spots missed. The OECD Recommendations then move to setting out principles and focus on the impact of AI rather than restricting the focus to a particular set of methods and techniques.

Similarly, the AHRCer in its 2021 report, "Human Rights and Technology" notes that the UN High Commissioner for Human Rights has advocated for a "smart mix" of regulatory measures to protect human rights in the context of AI. This means considering how human rights can be most effectively protected at each key stage of the AI lifecycle. The report lists the following stages: business and use-case development, design phase, training and test data procurement, building, testing, deployment, and monitoring.[19]

- **European Union**

In April 2021, the European Commission unveiled a new proposal for an EU regulatory framework on AI. The European Commission's proposed AI regulation is the world's first legislative framework on AI (the **EU AI Act**) – sets out rules for the development and use of AI systems in the European Union,[20] following a proportionate and risk-based approach. It establishes a definition of AI and a risk methodology to classify AI systems as (i) an unacceptable risk, (ii) a high risk, (iii) a limited risk, or (iv) a minimal risk, and lays down obligations that will apply to providers and users of high-risk AI systems. The regulation will be monitored by the Commission, which will establish a system for registering high-risk AI applications in a public EU-wide database.

The EU AI Act sets out a broad, pragmatic definition of AI systems as "software that is developed with one or more of the techniques and approaches listed in Annex I of the EU AI Act and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with" (Title I, Article 3).

The definition is likely to be subject to close scrutiny and possible amendment, but the European Commission clearly intends to cast a wide net, capturing not only AI systems offered as stand-alone software products, but also products and services relying on AI services directly or indirectly.

Mireille Hildebrandt considers that the condition that a system must achieve "human-defined objectives" may exclude ADM systems and automated decision-support (**ADS**) systems which is problematic as the output of ADM and ADS systems might still be based on the output of data-driven systems that learn and/or model. Hildebrandt argues that legal protection should depend on automation's potential impact rather than the specific techniques that have been employed to bring about that outcome or impact.[21]

- **United States of America**

In the US, no AI-specific legislation is currently in force, but there has been increased regulatory interest in AI, with the Federal Trade Commission releasing a statement that it would take enforcement action against biased AI systems under section 5 of the Federal Trade Commission Act. The Government Accountability Office has also issued a report on key practices to ensure responsible use of AI by federal agencies.

In addition, the 2020 Executive Order on AI guides federal agencies in taking up trustworthy AI in federal government.[22] Agencies are to use AI in a way that is: (a) lawful and respectful of America's values, (b) purposeful and performance-driven, (c) accurate, reliable, and effective, (d) safe, secure, and resilient, (e) understandable, (f) responsible and traceable, (g) regularly monitored, (h) transparent, and (i) accountable.

---

[19] AHRC, Human Rights and Technology (above, n 1) 45-46.

[20] Proposal for Regulation of the European Parliament of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM/2021/206) < https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>.

[21] Mireille Hildebrandt, 'Global Competition and Convergence of AI Law' (2022) *SocArXiv* 10 <https://doi.org/10.31235/osf.io/j36ke>.

[22] *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Executive Order 13960, 3 December 2020, 85 FR 78939) <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>.

In October 2021 the White House Office of Science and Technology Policy (**OSTP**) announced a plan to develop a "bill of rights" to protect individuals from potentially harmful consequences arising from AI applications developed using biometric data such as facial recognition, voice analysis, and heart rate trackers.[23] This is similar to a rules-based / outcomes-based approach that the NSWCCL submits should be adopted in Australia. The focus remains on biometric systems including tracking voice, gestures, heart rate, facial expressions and hiring software.[24]

- **Singapore**

The Monetary Authority of Singapore has partnered with industry to develop the fairness metric and assessment methodology for AI-led credit risk scoring and customer marketing. The 'Veritas Initiative' aimed to support the implementation of fairness, ethics, accountability and transparency (FEAT) principles developed by MAS in the use of AI by the financial sector. This is an example of developing industry guidance for implementing a government-endorsed AI ethics framework. It may be helpful to consider if the developed methodology can be leveraged in the Australian context for specific industries.

4. AUTOMATED DECISION MAKING

4. Introduction

Existing protections against ADM are insufficient as they are vague and outdated. In this regard, NSWCCL considers the Commonwealth Ombudsman's *Automated decision-making better practice guide* is no longer fit for purpose and lacks necessary oversight, review and enforceability provisions.

In particular, NSWCCL submits that there are currently only limited ways for individuals to challenge ADM decisions – this is especially so given individuals are often not even aware that ADM is being utilised in a decision-making process. The Attorney General's Department's Review of the Privacy Act Discussion Paper published in October 2021 recognised this limitation and sought stakeholder feedback on whether protections contained in GDPR (such as the right to explanation about the logic of ADM and the right to opt out of certain forms of ADM) should be transplanted in Australia. As outlined in our submission in response to that Discussion Paper, the NSWCCL supports the introduction of similar rights for individuals in the context of ADM. A copy of NSWCCL's submission to that Discussion Paper is appended as Annexure 1 below.

4. Proposed regulatory approach

- **Jigsaw approach**

NSWCCL considers that no single piece of legislation (such as the Privacy Act 1988 (Cth) alone) can adequately protect individuals from the existing and emerging risks of adopting ADM. Instead, a "jigsaw" regulatory approach must be adopted, comprising of:

- Privacy and data protection laws, human rights law, freedom of information, public law, administrative law, discrimination law, and consumer law; and

- New legislation targeted at regulating AI, such as the European Commission's regulatory framework proposal on AI.

NSWCCL submits that such legislation must go beyond the capacity for judicial consideration after the fact, or non-binding policy guidance. Huggins has noted that there are many judicial challenges when it comes to ADM, as "judicial consideration of individual cases has limited utility in addressing the systemic concerns associated with

[23] Eric Lander and Alondra Nelson. 'ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World (Online, 22 October 2021) <https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/>.

[24] Glenn Gow, 'The AI Bill of Rights: Protecting Americans from the Dangers of Articial Intelligence,' *Forbes* (Online, 9 January 2022) <https://www.forbes.com/sites/glenngow/2022/01/09/the-ai-bill-of-rights-protecting-americans-from-the-dangers-of-artificial-intelligence/?sh=189862727173>.

the use of automated systems".[25] Considering this, there is an argument to be made that there must first be widespread legislative reform to complement the necessary doctrinal evolution.

This possibility was discussed by the Australian Law Reform Commission, which proposed exploration of law reform options on the topic of ADM and administrative law in December 2019. To date, the Australian government has not done this. Instead, the Australian government, in response to ADM, has chosen only to issue non-binding policy guidance, such as the Administrative Review Council's *Automated Assistance in Administrative Decision Making and the Automated Assistance in Administrative Decision-Making: Better Practice Guide*. Against this, Huggins concluded that non-binding policy guidance is not, "in isolation, a sufficiently robust response to ensure the appropriate design and deployment of automated systems".[26] Given the high stakes associated with poorly design automated systems and their potential for eroding trust in government decision-making processes, there is a need to explore new legal frameworks to develop and control the issues around ADM and AI in government decision making.

The regulatory approach to ADM should include both:

- individual rights (for example, the right to an explanation under privacy law); and
- obligations on both government and non-government entities engaging in ADM to ensure, through robust procedures and safeguards, transparency and fairness, when using ADM.

Creating obligations on entities to uphold transparency and fairness, alongside other similar values, is crucial given the complexity and opaqueness of ADM. These complexities often prevent individuals from challenging unfair, incorrect or discriminatory decisions resulting from ADM, such as via traditional administrative law or discrimination law avenues. As such, considerations of fairness and transparency must be built in from the outset, such as data protection by design.

Notification and audit requirements for ADM

ADM is used by various government agencies such as Centrelink, Comcare, the Department of Defence, the Department of Veterans' Affairs and the Australian Tax Office.[27] In order to access necessary public services, vulnerable individuals are likely to engage frequently with government agencies and be subject to decisions made through ADM. Noting this, there is a great imperative to ensure adequate checks and balances exists around the use of ADM by government agencies in administrative decision-making. In the NSWCCL's view, it is best practice to ensure that when ADM is used, individuals are: (1) notified; (2) given access to a clear explanation of the logic and processes of the ADM; and (3) informed about the significance of the ADM and envisaged consequences. As noted in the Article 29 Working Party *Guidelines on Automated individual decision-making and Profiling*,[28] entities using ADM should "find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision", rather than only providing a complex explanation of the algorithms used or solely relying on disclosure of the full algorithm.

This information should be accompanied by an opportunity for individuals to obtain meaningful human intervention from someone who has the authority and competence to change the decision. Regimes that guarantee access to this information and opportunities for review foster greater transparency and accountability in the use of ADM.

The 'Human Rights and Technology' report, produced by the AHRC, recommended the Government introduce legislation requiring a human rights impact assessment (**HRIA**) be undertaken before any governmental agency or department uses ADM to make administrative decisions.[29] The HRIA should include public consultation and should assess whether the ADM:

(i) complies with Australia's international human rights law obligations;

[25] Huggins (above, n 14) 1052.
[26] Ibid, 1073.
[27] Administrative Review Council, *Automated Assistance in Administrative Decision Making: Report to the Attorney-General* (Report No. 46, November 2004).
[28] Available online: < https://ec.europa.eu/newsroom/article29/items/612053/en>.
[29] AHRC, 'Human Rights and Technology' (above, n 1) 55.

(ii) will involve automating discretionary elements of administrative decisions;

(iii) provide for appropriate review by human decision makers; and

(iv) is authorised and governed by legislation.

The report also suggests the Government introduce legislation to require notification to any affected individual when AI is materially used in making an administrative decision – with such notification to include the avenues through which an affected individual can challenge the decision – and that the Government should commission an audit of all current or proposed use of AI-informed decision-making by or on behalf of governmental agencies. NSWCCL supports these recommendations because they prioritise human rights and attempt to reduce the imbalance of power by placing obligations on the Government, when using ADM, to be fair, transparent, and held to account.

Regulator oversight

To ensure that the "jigsaw" approach is effective, the AHRC in its 'Human Rights and Technology' report of 2021 recommends the establishment of an AI Safety Commissioner as an independent statutory office, focused on promoting safety and protecting human rights in the development and use of AI in Australia.[30]

The NSWCCL also supports the establishment of an AI Safety Commissioner as a separate independent statutory office. We consider such an office should provide oversight for, and have powers to intervene (including by way of sanctions / penalties) in relation to the development and deployment of AI and ADM, and any AI or ADM specific legislation that may be passed. Although the existing office of the OAIC will have some overlap with a new AI regulator, the NSWCCL submits that the OAIC is already under-resourced and overburdened in the handling of privacy and freedom of information claims.

NSWCCL submits that a standalone AI Safety Commissioner is warranted having regard to the following:

- AI and ADM are emerging technologies with a wide suite of applications and potential risks and harms including for consumers, government and more broadly society).
- Effective regulatory oversight of ADM and AI is likely to require fundamentally different considerations and specialised skillsets to adequately monitor and regulate, in order to ensure consumers and society are safeguarded from emerging threats and risks. Regulatory oversight specific to AI and ADM will therefore require appropriate sanctions and enforcement powers.
- A stand-alone, specialised AI Safety Commissioner would be able to develop technical and regulatory capacity that will not only be able to provide an intervene in relation to AI / ADM specific legislation, but also assist other regulatory bodies in regulating AI and ADM related issues that are regulated under other existing legislative regimes.
- An AI Safety Commissioner may also increase public trust in the use of AI and ADM, as there would be dedicated / expert oversight of government use of AI and ADM, and a specialised body to which the general public can bring complaints. As illustrated by Robodebt, there are few, if any, accessible avenues of recourse available for individuals by AI and ADM harms.

In order to be effective, the NSWCCL submits that the AI Safety Commissioner must receive adequate resourcing, both in terms of funding and personnel. The Government released an AI Action Plan which includes a targeted $124.1 million investment over 2021-2022 to strengthen Australian leadership in developing and adopting responsible AI.[31] In the context of this phase of the AI Action Plan, it has placed its focus on supporting business adoption of AI. The NSWCCL submits that the responsible use and development of AI and ADM is dependent on directing some of that governmental support and funding towards the establishment of a separate AI Safety

[30] Ibid.

[31] 'Australia's Artificial Intelligence Action Plan', *Department of Industry, Science, Energy and Resources*, (Web Page, June 2021) <https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan/direct-ai-2021-22-budget-measures-implementation-and-next-steps>.

Commissioner, for the reasons outlined above. The adequate funding of an AI Safety Commissioner will allow it to develop its own capabilities side-by-side business and Government as these technologies and their range of applications continue to evolve.

Finally, with respect to jurisdictional oversight, consideration should be given to the creation of a single national AI Safety Commissioner with jurisdiction to oversee Commonwealth and State public agencies and private sector organisations. Most state government agencies are separately subject to their respective state regulators and state privacy and freedom of information legislation. Use of AI and ADM is relevant in both the public and private sector contexts on a state and federal level, and so a coordinated approach with state regulators is recommended.

- **Sanctions**

In recognition of the potential harm that misuse of ADM can result in, particularly when it comes to the impact on vulnerable populations as discussed further in section 2.4 below, NSWCCL submits that there should be significant sanctions attached to any breaches of regulation to encourage compliance. Sanctions can be provided for in legislation and regulations, and the OAIC should be able to issue sanctions as a result of any review or audit.

4. Law makers should draw upon international developments and regulatory models

Several jurisdictions overseas have introduced laws that contemplate and regulate the use of ADM. NSWCCL suggests that ADM regulation in Australia may be guided by these international developments. Of note are the EU General Data Protection Regulation (**GDPR**) and the California Privacy Rights Act (**CPRA**).

- **GDPR**

Huggins notes that, under the GDPR, there is a "suite of notification, access and explanation rights for individuals subject to automated decisions".[32] Firstly, governments that use automated processes must proactively notify any affected individuals of the existence of solely automated decision-making. Additionally, these government bodies must provide meaningful information about the logic of the decision-making process as well as the significance and possible consequences of such processing for an individual. Finally, individuals also have the right to request access to these forms of information that may impact them. Huggins notes that these provisions recognise that an individual can only challenge a particular decision or express their view if they understand how the decision was made and on what basis.[33]

The GDPR also includes the following requirements that we submit Australian lawmakers should consider:

- The GDPR requires that individuals be given prior notice of the use of personal data in ADM, including profiling. The GDPR also provides a right to access information regarding the existence of ADM and "meaningful information about the logic involved, as well as the significance and the envisaged consequences" of such processing to the individual.

- The significance of the human aspect in decision-making holds a critical place in the EU model. The GDPR contains a prohibition against "decisions based solely on automated processing", which have legal or similarly significant effects (e.g. decisions about credit, or employment), with certain noted exceptions. Further it explicitly recognises the enhanced protection required for vulnerable adults and children.[34]

- While there is an exception allowing decisions to be based solely on automated processing, Article 22 of the GDPR provides three safeguards to protect individuals. These require the data controlled to implement measures to safeguard: (i) the subject's right to express one's point of view; (ii) the subject's right to obtain human intervention; and (iii) the subject's right to contest the decision.

Relevantly, the AHRC has proposed similar protections in Australia, which would require notification to individuals when AI is materially used in making an administrative decision or a decision affecting the legal, or similarly

[32] Huggins, (above, n 14) 1075.

[33] Ibid.

[34] Available online: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/are-there-restrictions-use-automated-decision-making_en>.

significant, rights of an individual and include information about how to challenge the decision for administrative decisions materially made by AI.[35] The NSWCCL submits that individuals who are the subject of automated processing should have similar rights as those under the GDPR, which would allow them to obtain human intervention and contest the decision.

- **CPRA**

The CPRA establishes the California Privacy Protection Agency (**CPPA**) as an independent watchdog to enforce the law, perform an educational function for the public and provide technical assistance to the legislature with respect to privacy-related legislation as well. The CPPA will appoint a chief privacy auditor to conduct audits of businesses to ensure compliance with the CPRA.

- The CPRA will allow regulations to be developed by the CPPA to grant access and opt-out rights with respect to ADM technology and will require businesses' responses to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.

- The CPRA also creates consumer access rights that include access to information about inferences drawn "to create a profile". In line with the GDPR, the CPRA defines "profiling" as any automated processing of personal information "to evaluate certain personal aspects relating to a natural person, and in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

- The NSWCCL supports access, notification, and explanation rights in respect of personal information used in the context of ADM.

Yours sincerely,

Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission:

Stephen Blanks, Treasurer
Mobile: 0414448654
Email: stephen.blanks@nswccl.org.au

Michelle Falstein, Secretary
Mobile: 0412980540
Email: michelle.falstein@nswccl.org.au

[35] Australian Human Rights Commission, 'Human Rights and Technology' (above n 5) 60, 77-78.

Annexure 1

NSWCCL's response dated 9 January 2022 to the Discussion Paper published in connection with the Attorney General's Review of the Privacy Act

NSW Council for Civil Liberties Inc.
PO Box A1386, Sydney South,
NSW 1235, Australia

e: office@nswccl.org.au
t: 02 8090 2952
www.nswccl.org.au

@nswccl
@nswccl

ANNEX 2

NSWCCL SUBMISSION

ATTORNEY-GENERAL'S DEPARTMENT

PRIVACY ACT REVIEW – DISCUSSION PAPER

9 January 2022

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

The NSWCCL's response to the Attorney-General's Department Privacy Act Review- Discussion Paper

Introduction

The New South Wales Council for Civil Liberties (**NSWCCL**) thanks the Attorney-General's Department for the opportunity to make this submission in response to the Privacy Act 1988 (Cth) (the **Act**) Review Discussion Paper.

As we advocate throughout this submission, urgent reform is required to modernise the Act and ensure it is fit for purpose in the digital economy. Privacy is a fundamental human right that is central to the maintenance of democratic societies and achieving respect for human dignity. In this regard, the NSWCCL submits that the right to privacy should be the paramount object of the Act and considers the two primary areas of concern in debates relating to privacy are:

(a) the intrusive observation of one's actions (whether by surveillance, listening, data analysis or other mode); and

(b) the discussion and the misuse of personal information.

NSWCCL supports in-principle many of the proposals outlined in the Discussion Paper and commends the Attorney General's Department for reflecting the legitimate privacy concerns of a broad spectrum of society. Many Australians are concerned about gaps and ambiguities in the existing privacy regime that undermine the right to privacy. This is especially important in the context of unprecedented integration of digital technology in our everyday lives.

The NSWCCL provides this submission with a view to further refining many of the proposals outlined in the Discussion Paper to ensure that reforms to Australia's privacy framework are sufficiently protective of privacy and reflect the needs of individuals rather than the interests of business. Before delving into our specific feedback regarding the various proposals to modernise the Act, the NSWCCL would like to make the following overarching submission to be considered as this Privacy Act Review moves forward:

- Failure to properly protect privacy results in a reduction in human autonomy and freedom,[1] which can harm democratic processes. Enshrining the protection of an individual's right to privacy as the paramount object of the Act is an important initial step, but the NSWCCL considers that the introduction of a carefully considered definition of 'privacy' is of equal importance.

- The NSWCCL strongly agrees with the introduction of further organisational accountability requirements into the Act. In light of information and power asymmetries in the processing of personal information, individuals should not be expected to bear the burden of managing privacy risks themselves. Placing the burden of privacy protection onto the individual is unfair and impractical. It is the organisations that hold personal information – governments and businesses – that must bear responsibility for respecting the right to privacy.

- The expansion of the OAIC's funding is critical given that several proposals contained within the Discussion Paper involve the broadening of the OAIC's current remit. Chronic underfunding will erode the effectiveness of any privacy protections the OAIC seeks to implement and support. To properly conduct both its existing and proposed activities, the OAIC must be adequately funded and consulted in respect of the resources it requires. The OAIC received limited funding to support its privacy initiatives in the 2021-2022 Federal Budget, despite a significant expansion in its activities with the onset of its Digital Economy Strategy.

- There are some practices so privacy invasive or socially damaging that even putative 'consent' should not be allowed to authorise them. The OAIC has proposed introducing a "general fairness requirement for the use and disclosure of personal information" as a way of addressing "the overarching issue of power imbalances between entities and consumers" and "protecting the privacy of vulnerable Australians including children".

[1] Ziegler ed, *Human Rights and Private Law, Privacy as Autonomy*, 2007.

***Part One: Scope and Application of the* Privacy Act 1988**

1. OBJECTS OF THE ACT

Proposal 1.1: ***Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest as follows:***

a) to promote the protection of the privacy of individuals with regard to their personal information; and

b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest.

The NSWCCL supports the principle of enshrining the protection of an individual's right to privacy in the objects in section 2A of the Act, as privacy should not continue to be balanced in a way that favours commercial interests. However, we submit that the proposed amendments to section 2A do not go far enough to ensure an individual's right to privacy will be protected. The NSWCCL's position is that privacy law should extend beyond the regulation of handling personal information and should regulate fully the human right of privacy. To this end, and as noted in our submission in response to the Issues Paper, the NSWCCL supports the OAIC's suggested definition of what constitutes privacy, which we reiterate includes '*the right to be free from interference and intrusion, to associate freely with whom you want and to be able to control who can see or use information about an individual*'. We submit that such a definition should be considered, as it will assist in ensuring when actions or omissions by individuals or entities may be taken to cause privacy harm to an individual.

The objects of the Act in section 2A were developed in an environment in which privacy regulation was seen by big business as an obstacle. However, in 2021 privacy is not something to be balanced with commercial or business interests. Rather, it is of fundamental importance to individual autonomy and properly functioning democracy. Equally, the power of many commercial entities, including digital platforms, is such that there are legitimate dangers and concerns pertaining to democratic processes arising from the imbalance of power between individuals and companies that deal in data. The learnings of the Cambridge Analytica scandal are a significant lesson for all democratic countries in the importance of enshrining the protection of the privacy of individuals beyond only personal information.

Opting out of digital interactions is generally not realistic for most individuals, given the significant disadvantages, discrimination, and/or social exclusion that may eventuate for individuals who do not agree to terms of access. Given the power of certain digital platforms is such that there is an unassailable imbalance in the bargaining power between individuals and such entities, NSWCCL submits that the right to privacy should be enshrined as the paramount object of the Act. In this regard, we also submit that, while overlapping, the right to privacy extends beyond mere data protection and the concept of 'personal information', and that privacy law should reflect this conceptual distinction by accounting for additional aspects of privacy such as the right to freedom from intrusive observation. As a result, we reiterate that the absence of a substantive definition of privacy is a key shortcoming in the existing privacy regime, and that introducing a definition of privacy should be considered.

Separately, while we consider a public interest test may be a good mechanism to hold commercial entities to account with respect to their data collection and use practices, the NSWCCL submits that further consideration is required with regard to what entails the 'public interest' to ensure the intention of protecting an individual's right to privacy is realised. We agree that the subjective interests of entities are not relevant to the extent that their functions and activities are not in the public interest.[2] In the NSWCCL's view, the appropriate approach to reconciling the right to privacy with competing rights and interests is through a human rights legal framework, which recognises that

[2] Discussion Paper, 19.

different rights and interests may be in conflict and provides a methodology for balancing competing rights and interests. In this regard, the NSWCCL submits:

- It is preferable that express guidance is provided in the Act in the form of a carefully drafted definition of 'privacy'. Rather than specifying matters in the Act of what constitutes 'public interest', courts and decision-makers should have reference to how 'privacy' is defined within the Act. Under the existing privacy regime, the concept of 'Privacy' is the more uncertain concept, and greater statutory guidance is needed to understand what privacy entails to then determine what public interest should not encroach upon. The Act should therefore set out the values that the full human right of privacy seeks to protect. Any balancing test of proportionality or necessity will need to refer to these elements as against the relevant public interest consideration(s).

- If a public interest test is introduced, then the definition of 'public interest' must be broad and flexible to allow interpretations of the phrase to evolve over time and to account for various factual matrixes and contexts. 'Public interest' is a phrase that is used in various legislative instruments, and is therefore the subject of extensive judicial interpretation in various contexts. Courts [and other decision makers] are well placed to interpret the phrase with regard to precedent, whilst also tailoring it to the particular situation.

- The listing of specified matters that are to be considered in the 'public interest' should be avoided, given such specified matters will be subject to change with the passage of time. If, however, it is decided that a list should be included that sets out what 'public interest' should entail, the NSWCCL submits that the list should be non-exhaustive and avoid any reference to 'Australian values' given there have been instances in Australia's history where such values have not aligned with international standards of human rights (such as the White Australia policy). The legitimate struggles in other countries, such as apartheid in South Africa or the experience of slavery in many countries, also supports the view that the values of a society should not be incorporated into a public interest test. Further, from a practical perspective, the listing of factors to be considered in the public interest offers little guidance for context-specific assessments of how privacy should be balanced in a particular situation. If a list of factors is to be introduced, the NSWCCL would [support the Australian Law Reform Commission (**ALRC**) recommended definition of 'public interest' for the Act, which includes: '*freedom of expression, freedom of the media, the proper administration of government, open justice, public health and safety, national security, and the prevention and detection of crime and fraud*'.[3]]

- In addition, any balancing test that occurs should follow the guidelines of proportionality analyses developed through case law.[4] This is to ensure that, even if it is deemed that a public interest consideration outweighs the privacy interest at hand, any incursion on privacy must itself be undertaken in a balanced and proportionate way. We suggest the following considerations:

    - The interference must be deemed a legitimate public interest.
    - There must be a rational connection between the interference and the achievement of the public interest.
    - There must be no less intrusive but equally effective alternative.
    - There must not be a disproportionate burden imposed on the privacy rights-holder.

- Guidelines to ensure entities and individuals have a clear understanding of what data activities and functions are in the public interest may also assist. However, the NSWCCL considers further consultation is required with respect to when an APP entity will be taken to be acting in the public interest, to ensure the objects of the Act strike the right balance between privacy protection and public interest.

[3] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, September 2014) 152.
[4] One such analysis was undertaken in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Court of Justice of the European Union, C-131/12, ECLI:EU:C:2014:317, 13 May 2014) [97] where it was found that privacy rights "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name".

2. DEFINITION OF PERSONAL INFORMATION

Proposal 2.1: ***Change the word 'about' in the definition of personal information to 'relates to'***

The NSWCCL agrees that amending the definition of 'personal information' is critical to broadening the scope of application of the Act and modernising Australia's privacy regime. In particular, such a change will ensure that the Act captures the kinds of information that are processed by entities in a post-internet era, including technical information, allowing individuals to exercise greater control over their personal data.

Consequently, the NSWCCL supports the proposal to change the word 'about' to 'relates to' for the following reasons:

- First, this amendment would counteract the restrictive decision in *Privacy Commissioner v Telstra Corporation Ltd* 2017 FCAFC 4 ***(Grubb)***, in which the Court narrowly interpreted the concept of personal information, holding that an individual must be the subject matter of information for that information to be 'about' an individual and within the scope of the Act. The decision in *Grubb* is problematic because machines and technical data are increasingly the subject matter of information, rather than individuals themselves. For example, geolocation data or IP addresses are information about machines that connect to those cell towers or to an ISP. While these data are not 'about' an individual, such data can nevertheless be used to paint a detailed picture of an individual's life and impinge on their right to privacy. The effect of *Grubb* is to place these kinds of information outside the reach of the Act, significantly reducing privacy protections for Australians. By replacing the word 'about' with 'relates to', a greater range of information will be captured by the Act, including information linked to an individual by reason of its purpose or effect,[5] notwithstanding its apparently unrelated subject matter or content. This amendment is necessary to provide greater clarity to APP entities with respect to the types of information that should be afforded the protection of the Act, and to ensure the Act is adequate to respond to technological developments.

- Second, this amendment will bring Australia's definition of personal information in line with international data protection frameworks, such as the General Data Protection Regulation (**GDPR**) (which provides a definition of 'Personal Data' that includes the words 'relates to', and explicitly includes location data and online identifiers), the California Consumer Privacy Act (**CCPA**) (which defines 'personal information' to include online identifiers, IP addresses, account names, and similar identifiers), and in Canada (where courts have ruled that a broad range of technical information can amount to 'personal information', including IP addresses, RFID addresses, RFID tags, fingerprints, and video surveillance). Harmonising Australia's definition of personal information with modern international approaches to data is necessary to ensure Australians are afforded privacy protections that are fit for purpose in the digital age, while (in part) addressing efficiency concerns of global commercial entities that deal in data.

Proposal 2.2: ***Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.***

The NSWCCL generally supports the inclusion of a non-exhaustive list of the types of information capable of being covered by the definition of personal information, which we note can also be used to clarify the proposed expansion of 'personal information' in **Proposals 2.3 and 2.4** to extend to online identifiers, amongst other things.

The NSWCCL agrees with the list of technical information that could be capable of falling within the definition of personal information (as listed at page 27 of the Discussion Paper), which includes:

- an identifier such as a name;

- an identification number;

[5] *See, e.g. C-434/16* Peter Nowak v Data Protection Commissioner.

- location data;
- an online identifier; or
- one or more factors specific to the physical, physiological, genetic, mental, behaviours (including predictions of behaviours or preferences), economic, cultural or social identity, or characteristics of that person.

In addition to these factors, the NSWCCL submits that the following types of information should also be expressly included in the definition of personal information:

- information that can be inferred about the individual; and
- indirect information, such as information about an individual's family or associates.

Proposal 2.3: ***Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.***

The NSWCCL agrees with Dr Kemp's submission to the Issues Paper that the concept of identification should not be limited to data which is labelled with a person's legal name or contact details, but '*should extend to data which can be used to single out one consumer as distinct from other consumers*'. [6] In this regard, we agree with Dr Kemp that the use of strategies which single out unique individuals and create a detailed picture of '*the consumer behind the device' exposes individuals to tangible risks of 're-identification, manipulation, exclusion and discrimination*'.[7]

The NSWCCL therefore supports the proposal to include an additional definition in the Act that outlines when an individual will be 'reasonably identifiable' (i.e., a definition that clearly articulates the circumstances in which an APP entity or a third party could directly or indirectly identify anyone).

In this regard, the NSWCCL also supports a definition that would expressly include inferred personal information and considers that including the phrase 'directly or indirectly' would make it clearer to APP entities that they should consider other information available when assessing reasonable identifiability. A list of objective factors could also be included to assist APP entities in assessing whether an individual is indeed 'reasonably identified'. However, careful consideration of these factors is required to ensure the paramount importance of an individual's right to privacy is not undermined. The NSWCCL suggests the following factors for consideration, noting that if any list is included in the Act, it should be stated to be non-exhaustive:

- Taking account of all methods reasonably likely to be used by the APP entity or any other person in order to identify the individual, such as 'singling out'.
- The time and cost involved in identifying the individuals, and the operational capacity and resources of the entity that acquires the information.
- The available technology at the time of the processing and technological developments.
- The nature and specificity of the information, having regard to the context. For example, a common surname would not be reasonably identifiable of an individual in the context of a national population, but it would be in the context of a classroom of students.

The NSWCCL is concerned that by holding that information is only 'personal information' within the scope of the Act if it is 'about an individual', the *Grubb* case excludes indirect identification. In that case, Grubb was refused access to his internet browsing histories (URL addresses visited), assigned IP addresses, and geolocation (cell tower) data. The application of this case allows APP entities to conclude that such 'technical information' is not 'personal

[6] Submission to the Issues Paper: Dr Katharine Kemp, 11.
[7] Ibid.

information', because it only indirectly identifies an individual, and therefore doesn't receive privacy protection under the Act.

Including indirect identifiability within the definition of 'Reasonably Identifiable' would also bring the Act into line with international standards. The NSWCCL submits that the definition of 'Reasonably Identifiable' should be supported by guidance that draws on international case law and guidance, including from the GDPR, the CCPA, and Canadian courts, which define 'personal information' as including information that indirectly identifies an individual. Importantly, international jurisprudence has highlighted the ease with which information held by one entity can be combined with other information held by third parties to identify an individual. In this regard, we note:

- Although America's privacy regime is different from Australia's, there are helpful cases on 'mosaic theory', which is the concept that the aggregation of metadata can create a much more privacy-invasive picture than the individual instances of each data entry. *Carpenter v United States*[8] is illustrative of how geolocation information, which is generated when a mobile phone communicates with a cell tower, in combination with other information, can be used to identify an individual and generate a detailed picture of a person's movements and life. The Supreme Court of the United States held that a warrant was necessary for police to access the suspect's geolocation data. It amounted to saying that geolocation data, which is inferred information, should receive some form of privacy protection.

- Further, the Canadian Federal Court held in *Gordon v Canada (Health)* that information is 'about an individual' if it 'permits' or 'leads' to the possible identification of the individual, whether based on that information alone or in conjunction with other information.

- In relation to the GDPR's predecessor, the Court of Justice (**CJEU**) has favoured a broad and privacy-protective interpretation of the concept of identifiability. In *Breyer v Bundesrepublik Deutschland*, the CJEU considered whether a website visitor's dynamic IP address constitutes personal data, when a third party (an internet service provider) can tie a name to that IP address. The CJEU found that an IP address constitutes personal data when the website publisher has legal means to obtain additional data from the relevant ISP that enables the publisher to identify that visitor. This was a broad interpretation of the relevant provision that a person could be indirectly 'identifiable' and illustrates how assessment of identifiability should take into account the means likely reasonably to be used by the entity or any other person.

Proposal 2.4: ***Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.***

For the APPs to apply to an APP entity in relation to personal information, that personal information must first be 'collected'. Personal information 'relating to' an individual, or where an individual is only indirectly identifiable, is often inferred or generated. Accordingly, to ensure that the implementation of **Proposals 2.1 to 2.3** is given full effect, NSWCCL submits that the definition of 'collection' should be amended to include information obtained from any source and by any means.

Inferred information, such as location data, can be extremely revealing, and may amount to an invasion of an individual's privacy. The ACCC Digital Platforms Inquiry Final Report states that location data can be collected or inferred in many ways, including GPS, IP address, cell towers, Wi-fi access locations, and a user's mobile operator or ISP.[9] Given the *Grubb* case and its narrow interpretation of 'personal information', the NSWCCL supports clarifying that inferred and generated information fall within the protective scope of the Act by explicitly including inference as a means of collection, in conjunction with the widening of the scope of 'Personal Information' to include indirect identifiability (Proposal 2.3).

[8] No. 16-402, 585 U.S._____(2018)

[9] ACCC, *Digital Platforms Inquiry* (Final Report, June 2019) 385.

OAIC guidance states that 'collection' includes generating personal information from other data already held, such as the generation of an audit log.[10] As such, the NSWCCL considers that explicitly including the generation of personal information in the definition of 'collection' would more clearly align the Act with OAIC guidance and assist with application and enforceability of the Act.

As provided for by APP 5, such collection would need to be notified to individuals, and entities should have to specify how inferred and generated information might be collected and used. As acknowledged by the OAIC in its guidance on privacy in relation to data analytics, providing effective notice to individuals is difficult. In part, this is because APP entities often do not know what data they have or do not anticipate what they might generate. Further, data collection does not always arise from a specific transaction. This often results in the use of general privacy notices to facilitate extensive data collection communications (which is not best practice). In accordance with notification of data collection best practices, the NSWCCL supports the use of new technologies to give notice that is timely, concise, understandable, and meaningful. One example is the use of 'just-in-time notices', which appear at the point where individuals input personal information and provide a brief explanation of how the information they are about to provide will be used. The NSWCCL's position on giving notice is set out in greater detail in the response to Proposals 8.1 and 8.2 below.

Proposal 2.5: ***Require Personal Information to be anonymous before it is no longer protected by the Act.***

The NSWCCL supports Proposal 2.5 and considers the Act should be amended to require information to be 'anonymous' rather than 'de-identified' for the Act to no longer apply to that information. This more stringent standard of anonymity will enhance privacy protection by ensuring information that is merely 'de-identified' falls within the protective scope of the law.

Researchers from the University of Melbourne have shown how easy it is to re-identify individuals based on '*a few mundane facts*'.[11] They took de-identified, longitudinal medical billing records of 10% of Australians published by the federal Department of Health and were able to re-identify patients by linking unencrypted parts of the records with known information about the individuals. De-identification is unlikely to work for rich datasets like these. However, this kind of data should still receive privacy protections where it falls short of the standard of anonymisation to ensure personal information and privacy is protected.

The NSWCCL notes that the GDPR requires anonymization before privacy protections no longer apply to personal data. Under Recital 26, pseudonymised data is still considered information on an 'identifiable natural person', meaning it is still protected by the GDPR. Only where the data has been anonymised, such that the data subject is no longer identifiable, will the protections of the GDPR cease to apply. Determination of whether a natural person is identifiable must take into consideration all the means reasonably likely to be used either by the entity controlling the data or by another person to identify the natural person 'directly or indirectly' (as noted above).

In order to make anonymisation meaningful, NSWCCL considers that it may be helpful to adopt a definition similar to the GDPR's definition that anonymised information is '*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable*'. This would bring Australia in line with international standards and would clarify the distinction between de-identification and anonymisation.

Since anonymisation techniques will continue to evolve, and we should continue to encourage their development to aid in the protection of individuals' right to privacy, the NSWCCL submits that it may be restrictive to attempt to prescribe a standard for anonymisation within the Act itself. Accordingly, we suggest that OAIC should develop and release guidance (which it continues to monitor and update), which refers to international standards for the anonymisation techniques that provide appropriate protection without being so onerous that entities would be unable or unwilling to apply them.

---

[10] Office of the Australian Information Commissioner, *Chapter B: Key Concepts* (Web Page, 22 July 2019) < https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts#collects> B.28.

[11] Chris Culnane, Benjamin Rubinstein and Vanessa Teague, 'Health Data in an Open World' (2017) < https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf> 2.

The NSWCCL also considers this proposal a necessary change in order to support **Proposals 2.1 to 2.3**. This is because an expanded definition of 'personal information' will necessarily require more to be done to anonymise information so it falls outside that definition. The NSWCCL also agrees that the word 'anonymous' is more likely to send a clear signal to APP entities that they are required to meet a higher, irreversible standard.[12]

The NSWCCL recognises arguments that such changes may result in a chilling effect on research done in the public interest. However, the NSWCCL submits that the appropriate balance can be struck by requiring any intended and possible publication to be included as part of the consent form presented to the subjects of the research. We note that this is a standard research ethics requirement and is relatively uncontroversial. If the subjects do not give their consent to the publication of the research, their data cannot be published. It should, however, be open to entities to offer their research subjects a method for disseminating the results of such research in a way that protects an individual's right to privacy. For example, entities may be allowed to ask their research subjects to consent to the publication of their results after applying differential privacy techniques to the data set.

Proposal 2.6: ***Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.***

The NSWCCL does not support re-introduction of the *Privacy Amendment (Re-identification) Offence Bill 2016* (**Re-identification Bill**).

The Re-identification Bill was introduced in 2016 to address privacy violations that occurred in relation to data released by the Government. While criminalisation of malicious re-identification of publicly released data is in the spirit of attempting to increase privacy protections, the origins of the Re-identification Bill were a response to a particular situation that resulted in a blunt instrument that was not fit for purpose. Criminalisation in this instance operates as a last resort, as it is designed to threaten and deter re-identification. It does little to address the complex concerns surrounding general re-identification of data, which need to be addressed.

The NSWCCL submits that it is far more effective and sustainable for Australian government agencies and private sector entities to adopt a 'data minimisation' approach, as suggested by the Australian Privacy Foundation.[13] This approach requires that personal information is only collected where it is absolutely necessary by introducing data minimisation rules alongside penalties and compensation in the event of data breaches. Instead of targeting those undertaking re-identification – who may be third parties and outside Australia, making them difficult to prosecute – data minimisation encourages systemic change, incentivising entities to improve their data security and privacy protection measures. Targeting those who re-identify data does not do anything to encourage the entities responsible for de-identification and anonymisation to improve their processes and techniques. Nor does it provide any avenues of redress for those who have suffered a breach of their privacy rights. Further, promoting a data minimisation approach may also provide a better way to discourage offshore entities from re-identifying data.

However, should the Re-identification Bill be re-introduced, the NSWCCL submits that the following amendments should be incorporated:

- The Bill should apply to both de-identified and anonymised data.

- The Re-identification Bill should not apply retrospectively to 29 September 2016 as it was originally intended. Retrospective offences are incompatible with Article 15 of the International Covenant on Civil and Political Rights (**ICCPR**). The Attorney General's Department previously argued that retrospectivity was necessary to address a gap in existing legislation, and that it was appropriate due to the short period of retrospectivity. However, with the Re-identification Bill having lapsed, it should certainly not apply retrospectively to 2016, and the justification in the way of urgency to fill a legislative gap is further weakened with the passage of time.

- There should be greater clarification around the position of researchers who are not part of government agencies – this may comprise the potential inclusion of an exemption. As it stands in the Bill, the only recourse for

[12] Discussion Paper, 30.

[13] Australian Privacy Foundation, Submission No 11 to Senate Legal and Constitutional Affairs Committee, *Privacy Amendment (Re-identification Offence) Bill 2016* (16 December 2016) 2.

independent researchers is to apply to the Minister for an individual exemption. To counteract the potential chilling effect on research, including cyber security research, the Re-identification Bill should make clear the position on independent researchers.

- The Re-identification Bill should not reverse the onus of proof in requiring entities to prove that their behaviour was consistent with the relevant defences. The NSWCCL supports the Law Council of Australia in their submission on the Re-identification Bill that there is insufficient justification for the reversal of the onus. In particular, the matters to be established in court would not be extremely difficult or expensive for the prosecution to prove as they would have access to the relevant documentation.[14]

3. FLEXIBILITY OF THE AUSTRALIAN PRIVACY PRINCIPLES (APP)

Proposal 3.1: ***Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney-General:***

- ***where it is in the public interest to do so without first having to seek an industry code developer; and***
- ***where there is unlikely to be an appropriate industry representative to develop the code.***

The NSWCCL supports this proposal to empower the Information Commissioner (**IC**) to be able to develop an APP code without the direction of the Attorney-General, provided appropriate oversight mechanisms are introduced alongside it.

The lack of an industry code developer or an appropriate industry representative should not mean that an industry should go without a code where Australians are likely to benefit from a code being developed. An APP Code could provide greater clarity regarding the application and interpretation of the APPs and specific privacy issues that arise for APP entities in particular industries. Given the intrusions on an individuals' right to privacy can be incredibly context-specific, we suggest that an APP Code must be carefully tailored by the IC in consultation with various stakeholders. However, NSWCCL also considers that there must be appropriate oversight of this power because the potential to alter the APPs, which have been agreed upon by Parliament, may result in the inadvertent or deliberate removal of some of those privacy protections.

Allowing the IC to make an APP code is in line with powers afforded to the equivalent office in other comparable jurisdictions (the UK and New Zealand).

- The UK regime statutorily prescribes specific codes that the Commissioner must create, including an age-appropriate design code, data protection code, and journalism code. It requires the Commissioner to submit the final version of the code to the Secretary of State and Parliament for their approval.

- By contrast, the New Zealand regime does not require Parliamentary oversight – instead, it is based on public notice and allows for public submission. It allows the Commissioner to issue a code of practice on their own initiative, but the Commissioner must give public notice of their intention to do so and include a statement that the details of the proposed code may be obtained from the Commissioner, and submissions on the proposed code may be made in writing to the Commissioner within a specified period.

The NSWCCL submits that amendments to the Act to empower the IC to make an APP code should strike a balance between these international positions, and that favouring the requirement for Parliamentary approval in order to strengthen the oversight mechanism is preferable given that the power is intended to allow the development of a code without the need to seek an industry code developer. We also suggest that the following safeguards be implemented:

- parliamentary approval of any APP code to be developed (noting mere approval by the Attorney-General would be insufficient);

[14] Law Council of Australia, Submission No 10 to Senate Legal and Constitutional Affairs Committee, *Privacy Amendment (Re-identification Offence) Bill 2016* (16 December 2016) 9-10.

- adequate public consultation processes to ensure civil society, businesses, and the public have ample time to provide feedback on the APP Code); and

- the Act should provide general guidelines regarding the scope of IC-created codes, such as certain aspects of the APPs that cannot be derogated from.

Proposal 3.2: ***Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.***

The NSWCCL does not support Proposal 3.2 which would empower the IC to issue a temporary APP code on the direction or approval of the Attorney-General without Parliamentary approval, as this would subvert the role of Parliament and is a power that could be abused. The NSWCCL considers that there are existing emergency powers available to the Attorney-General that are curtailed with appropriate safeguards, which further supports the view that this proposal is both unnecessary and could be subject to abuse.

However, to the extent this power is to be introduced, the NSWCCL submits that oversight mechanisms must also be built into the Act to ensure the power can not be abused. Some suggestions in this regard include:

- a requirement for a sunset provision for the temporary code of a maximum of 12 months;

- an obligation on the Attorney-General to scrutinise and report on the effect of the temporary code;

- the obligation for the IC to give adequate public notice of the intention to issue a temporary code and make clear where the details of the code may be obtained; and

- strict requirements for the temporary code to be necessary and proportionate to the situation.

In addition, the NSWCCL submits that there must be strict guidance in the Act as to what 'urgently required' means in order to lessen the chances of abuse occurring. Any consideration of the 'public interest' must also be balanced against the definition of 'privacy' by way of a proportionality analysis, as submitted by NSWCCL above in response to **Proposal 1.1**.

Proposal 3.3: ***Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:***

- ***entities, or classes of entity***

- ***classes of personal information, and***

- ***acts and practices, or types of acts and practices.***

The NSWCCL supports this amendment, subject to the amendments ensuring greater specificity regarding the nature of the 'targeting' within Part VIA of the Act and the implementation of certain safeguards.

It may be envisaged that targeting Emergency Declarations would help to protect against privacy harms by removing generality of application. However, the ability to isolate certain entities and classes of personal information may actually facilitate the removal of privacy protections in a more in-depth way, as such removal may be considered proportionate and justified due to the lack of general application.

Accordingly, the NSWCCL submits that the following safeguards should be implemented:

- Parliament should have the power to disallow an Emergency Declaration;

- the Government's plans in relation to the Emergency Declaration and the targeting should be made publicly available, such as by displaying those plans on a website; and

- the proposed sunset clause in the Act, which is set at 12 months, should be amended to no more than 6 months in order to bring the Act in line with s 48 of the *Biosecurity Act 2015* (NSW) and could be brought down to 3 months in line with s 443(4)(b) of the *Biosecurity Act 2015* (Cth).

Proposal 3.4: ***Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.***

The NSWCCL supports this amendment, subject to the implementation of strict controls and safeguards. This is particularly so because of the meaning of 'permitted purpose' in Part VIA of the Act in relation to when information can be collected and used. In this regard, we note one permitted purpose listed in s 80H(2)(c) is '*assisting with law enforcement in relation to the emergency or disaster*'. The NSWCCL submits that sharing personal information for law enforcement purposes is not appropriate and that this permitted purpose should be removed from the Act, given the sharing of personal information amongst law enforcement agencies when an Emergency Declaration is in force is a slippery slope that risks impinging individuals' right to privacy and due process. Rather, the permitted purposes should be limited to the proper handling of the emergency, such as the provision of medical care and essential supplies, or ensuring that public safety is maintained.

While data sharing between organisations in emergencies can save lives and ameliorate the effects of disaster situations, we note that organisations may have more information on certain groups of people who are hesitant to share their information with the Federal government, such as Indigenous Australians. This simultaneously raises the potential for certain harms to occur due to sharing data with State agencies, which may disproportionately harm vulnerable groups in society.

To protect against those harms, the NSWCCL submits appropriate safeguards should be built into the Act, including:

- data collected pursuant to an Emergency Declaration should not be capable of being used in the course of any potential prosecution by the State, either during or subsequent to the period of the Emergency Declaration;

- data collected pursuant to an Emergency Declaration should not be shared for law enforcement purposes, even when assisting in relation to the emergency or disaster;

- strict controls setting out the kind of information that will be shared between the state/territory agencies;

- strict controls regarding the retention of information beyond the period of the Emergency Declaration and outlining the return or destruction of information;

- public declarations stating that there is an Emergency Declaration in force and the details of the Emergency Declaration, including the organisations and agencies that are sharing information; and

- a potential restriction that information can only be shared if it was given after the implementation of this amendment.

4. SMALL BUSINESS EXEMPTION

Though there was no specific proposal in connection with the exemptions in the Discussion Paper, views as to alternative options appropriate in the Australian context have been sought.[15] The NSWCCL reiterates its support for alternative 1 that the small business exemption be removed.[16] Further, the NSWCCL opposes any exemption based on turnover thresholds.

[15] Discussion Paper, 44

[16] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1358

The Discussion Paper refers to the GDPR adopted risk-based approach, which the NSWCCL considers is better calibrated to shifting privacy law towards substantive protection of fundamental rights and freedoms.[17] We suggest this approach deserves further consideration moving forward.

5. EMPLOYEE RECORDS EXEMPTION

The NSWCCL supports the first suggested approach in the Discussion Paper for the removal of the employee records exemption and refers to comments made in its previous submission.

6. POLITICAL PARTIES EXEMPTION

The NSWCCL supports removing the exemption for political parties and refers to comments made in its previous submission.

The NSWCCL preferred position, having advocated for removal of the s6C exemption, is that the limited exemption for acts and practices of political representatives and contractors in s7C should also be removed.

7. JOURNALISM EXEMPTION

The NSWCCL supports the retention of the journalism exemption. To balance the protection of privacy rights with the important role of journalism in a democratic society, a more restrictive definition of 'journalism' should be introduced limiting the scope of the exemption to acts and practices that are associated with a clear public interest in the freedom of expression.[18]

It is inappropriate for the Act to introduce a requirement for journalism to be in the 'public interest' to be protected. Further, the Act ought to refrain from defining the types of journalism that is in the 'public interest'.

A preferable approach is to define the public interest as one of freedom of expression. Community expectations are that the media should respect individual privacy. However, new technologies have resulted in the proliferation of new non-traditional media and increasingly pervasive forms of journalism. The NSWCCL supports the adoption of the test laid down by the Court of Justice of the European Union (**CJEU**) in *Buivids* that journalistic activity must be '*intended solely to disclose information, opinions or ideas to the public*' [62]. With a secondary element that a Court must consider '*whether the exemptions or derogations provided for … are necessary in order to reconcile the right to privacy with the rules governing freedom of expression, and whether those exemptions and derogations are applied only in so far as is strictly necessary*' (at [68]). This appropriately balances the public's interest in freedom of expression through journalism and individuals' right to privacy. There is no principled reason for drawing a distinction between citizen journalists and those employed by media organisations. The NSWCCL accepts that not all content uploaded to the internet falls within the journalism exception, and considers the CJEU's approach to be best practice in relation to the protection of journalism.

[17] Discussion Paper, 43

[18] ALRC Report No 108 Retaining an exemption for journalistic acts and practices

Part Two: Protections

8. NOTICE OF COLLECTION OF PERSONAL INFORMATION

Proposal 8.1: ***Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.***

Proposal 8.2: ***App 5 notices limited to the following matters under APP 5.2:***

- ***the identity and contact details of the entity collecting the personal information***
- ***the types of personal information collected***
- ***the purpose(s) for which the entity is collecting and may use or disclose the personal information***
- ***the types of third parties to whom the entity may disclose the personal information***
- ***if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection***
- ***the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and***
- ***the location of the entity's privacy policy which sets out further information.***

The NSWCCL supports the introduction of an express requirement in APP 5 that privacy notices must be clear, current and understandable (**Proposal 8.1**).

The NSWCCL also supports the inclusion of the types of information set out in **Proposal 8.2**, including the identity and contact details of the entity, the types of personal information collected, the purposes for which the entity is collecting personal information and interaction with third parties. Provision of clear, detailed and actionable information is particularly important in allowing expert intermediaries, such as privacy advocates, to obtain sufficient information to inform non-experts of the effects of data practices.

We note the overlap with the requirement that all notices be clear and understandable, current, and provided in a timely manner, to be included in the Online Privacy Code, enabled by the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill* 2021. An important component would be to ensure that the Notices provide an adequate level of specificity, to make clear to consumers what kind of information is collected.

The NSWCCL also notes that the Bill's Regulatory Impact Statement found that Privacy Policies are '*often vague, lengthy, legalistic and difficult to comprehend*'. The opposite is frequently true of Privacy Notices, which provide insufficient detail as to the specific kinds of personal information collected and what is done with this information.

While an important component of rendering Notices 'understandable' is that they use simple and plain English, a Notice is not 'understandable' to a consumer where its language is too broad to make clear the specific kinds of information collected. However, in order to mitigate the risk of 'overloading' individuals with information, the notification interface should be managed to provide brief and concise notification, which permits more concerned users to access further information.[19] For example, a notification could list types of third parties to whom consumer's information is disclosed, and provide a hyperlink to a more detailed list of actual third parties.[20]

[19] Katharine Kemp and Rob Nicholls, Submission to Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report'* (1 March 2019) 6 < https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf>.
[20] Ibid.

Proposal 8.3: ***Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.***

Proposal 8.4: ***Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:***

- ***the individual has already been made aware of the APP 5 matters; or***
- ***notification would be impossible or would involve disproportionate effort***

The NSWCCL supports the use of standardised privacy notices, to aid consumer comprehension and to ensure that the notices provide clear and understandable information (**Proposal 8.3**). As some submissions to the Issues Paper noted, a standard format could help consumers develop expertise in reviewing and understanding data collection policies, while limiting 'information overload'.

The NSWCCL submits that notification of collection should be required prior to the time of collection (**Proposal 8.4**). Individuals must also be given the opportunity to review and understand the notice, and exercise their right to object.

9. CONSENT TO THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Proposal 9.1: ***Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.***

Proposal 9.2: ***Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.***

The NSWCCL supports the clarification of the definition of consent in the Act to establish criteria for valid consent (**Proposal 9.1**)**.** The NSWCCL agrees that consent should be freely given, informed, current, specific and an unambiguous indication through clear action. Further, the NSWCCL supports the use of standardised consents to ensure that consents are clear, effective and understandable for consumers (**Proposal 9.2**). Entities should bear the burden of proving that valid consent has been obtained where consent is given because services are often offered on a take-it-or-leave-it basis, that is, where the provision of services is conditioned on consent, this is not valid or meaningful consent.

The NSWCCL is particularly concerned about the ability for users to give meaningful consent, given information asymmetries, the lack of choice in terms of privacy settings, and the problem of consent fatigue.

Consumers' ability to make informed choices is affected by '*information asymmetry between digital platforms and consumers'* and the *'bargaining power held by digital platforms compared to consumers*'.[21] In particular, the '*length, complexity and ambiguity of online … privacy policies*' alongside the use of '*standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents*' impede on consumers' ability '*to provide well-informed and freely given consent to [the] collection, use and disclosure of their valuable data*'.[22] A review of certain digital platforms' terms of use and privacy policies reveals that simply by signing up to a digital platform, a consumer has signalled their acceptance of the platform's privacy policies and crucially, acceptance of terms that allow most of these platforms to *unilaterally* vary their privacy policies from time to time.[23]

[21] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 23 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

[22] Ibid.

[23] Ibid 395.

NSWCCL also notes that care must also be taken so that 'consent fatigue' is minimised.[24] This may involve '*not requiring consent when personal information is processed in accordance with a contract to which the consumer is a party, or using standardised icons or phrases … to facilitate consumers' comprehension and decision-making*'.[25]

Contrary to claims of a 'privacy paradox'[26] — that is, the notion that consumers' revealed preference is actually a lack of concern for privacy — where consent is given in response to terms offered on a take-it-or-leave-it basis, such an argument cannot be supported. The relevant consumer behaviour in this context is not derived from a 'privacy paradox' per se but rather the fact that consumers are incapable of making an informed choice due to concealed data practices.[27]

For consent to be meaningful, the NSWCCL considers that there ought to be an obligation on suppliers of services to offer different levels of services conditioned on the choices made by consumers in relation to dealings with their personal information. Crucially, these must not be artificial choices that have the same practical effect of a take-it-or-leave-it option. What this creates is an incentive for consumers to not only read their privacy information but also make a conscious choice about how they wish to have their information used.[28] After all, '*[t]he likelihood of reading is also influence[d] by the extent to which consumers are incentivised to read communications — if consumers cannot exercise any options on privacy as a result of communications, other than to walk away from a contract, they have little reason to read them*'.[29]

Ultimately, '*[a] "take it or leave it contract" only provides a net benefit to the reader where the reader decides on balance to walk away from it. Where the consumer has already decided to acquire or use a particular product or service, the consumer has little reason to read privacy information that cannot be acted upon*'.[30] Moreover, with the way in which modern day consumers are now reliant on online services, '*it may be unreasonable to argue that consumers who are unhappy with a business's contract terms services should simply "walk away"*'.[31]

The quality of consumers' consent may be raised by increasing the 'actionability' of the terms and conditions — that is, by 'encouraging consumers to actively participate in, rather than passively accept, the terms and conditions surrounding the use of their personal information.[32] The more options given to consumers about how their information will be used, the more engagement and consequently better and more informed decisions.

Furthermore, consent cannot be allowed as a substitute for failure to provide minimum consent standards. As such, the NSWCCL supports a proposal for the Australian Consumer Law (**ACL**) to be amended so that consent is not sufficient to authorise data practices which would otherwise be unfair, discriminatory or might cause significant harm to an individual.

---

[24] Ibid 35.

[25] Ibid.

[26] See, eg, Bettina Berendt, Oliver Günther and Sarah Spiekermann, 'Privacy in E-Commerce: Stated Preferences vs. Actual Behavior' (2005) 48(4) *Communications of the ACM* 101; Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours' (2007) 41(1) *The Journal of Consumer Affairs* 100; Spyros Kokolakis, 'Privacy Attitudes and Privacy Behavior: A Review of Current Research on the Privacy Paradox Phenomenon' (2017) 64 *Computers & Security* 122.

[27] Katharine Kemp and Rob Nicholls, Submission to Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (1 March 2019) 3 <https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf>.

[28] Jeremy Riddle, 'Consumer Concerns: Informing Consent Online and Empowering consumers through Better Communication of Privacy Information' (2017) 25(2) *Australian Journal of Competition and Consumer Law* 149, 152.

[29] Mark Briedis, Jane Webb and Michael Fraser, *Improving the Communication of Privacy Information for Consumers* (Report, February 2016) iv <https://accan.org.au/files/Grants/Improving%20Comm%20Privacy%20Info_web.pdf>.

[30] Ibid 51.

[31] Ibid iii.

[32] Jeremy Riddle, 'Consumer Concerns: Informing Consent Online and Empowering consumers through Better Communication of Privacy Information' (2017) 25(2) *Australian Journal of Competition and Consumer Law* 149, 152, discussing Mark Briedis, Jane Webb and Michael Fraser, *Improving the Communication of Privacy Information for Consumers* (Report, February 2016) <https://accan.org.au/files/Grants/Improving%20Comm%20Privacy%20Info_web.pdf>.

10. ADDITIONAL PROTECTIONS FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Proposal 10.1: ***A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.***

The NSWCCL is supportive of an objective standard for when and how personal information may be collected and disclosed, and considers that such collection, use or disclosure of personal information must be fair and reasonable in the circumstances, even if an individual consents to collection. As stated in the NSWCCL's submission to the Privacy Act Review Issues Paper, the NSWCCL does not support overreliance on the Notice and Consent model used to collect, use and store data in Australia – regulators must impose standards for collection that go beyond whether collection is consented to, especially in light of problems identified in response to **Proposals 9.1** and **9.2** regarding the lack of meaningful consent, as well as the need for (and NSWCCL's support of) clear notice of collection (**Proposal 8.1**).

However, any amendment should make clear that any privacy notices provided by the APP entity in relation to proposed collection and use of personal information will not change the standard of what is '*fair and reasonable in the circumstances*'. In practice, whether it is 'fair and reasonable' for an APP entity to collect, use, and disclose personal information should be informed in the circumstances by reference to the nature and purpose of collection or use. This assessment should not be reliant on the individual having carefully read broadly-worded privacy notices provided by the APP entity or require the individual to have the capacity to meaningfully engage with such privacy notices so as to exercise their informed consent.

The NSWCCL considers that the proposed text could make clearer that the 'fair and reasonable' standard is intended to operate by reference to the reasonable expectations of the individual, rather than the APP entities themselves. We note this is contained in the legislated factors (Proposal 10.2), but consider that such consideration could be made paramount by amending the text to read: '*fair and reasonable in the circumstances, as considered from the perspective of a reasonable person in the place of the individual user*'. This combines the objective element contained in Canada's PIPEDA standard for personal information collection (that 'a reasonable person would consider appropriate in the circumstances': s 5(3)) with the GDPR's focus on the user's position (which requires personal information be collected fairly 'in relation to the data subject': art 5(1)). The NSWCCL's concern is that — as the proposal currently stands — the language is broad enough that 'fairness' may be judged

from the APP entity's perspective, and therefore may allow consideration of purposes of collecting personal information that are not apparent to users.

Proposal 10.2: ***Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:***

- ***whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances;***
- ***the sensitivity and amount of personal information being collected, used or disclosed;***
- ***whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information;***
- ***whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity;***
- ***whether the individual's loss of privacy is proportionate to the benefits;***
- ***the transparency of the collection, use or disclosure of the personal information; and***
- ***if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.***

The NSWCCL supports the inclusion of non-exhaustive legislated factors that are relevant to determining whether the collection, use, or disclosure of personal information is fair and reasonable in the circumstances. However, it considers that clear guidance and examples of how these factors may apply in practice must be provided.

The standard of 'fair and reasonable' must be assessed by reference to the perspective of the individual, rather than being assessed from an APP entity's perspective. We consider that having clear guidance from the outset, rather than waiting to see how the courts interpret such new provisions, will empower APP entities to appropriately assess whether any proposed data collection, use or disclosure would be unfairly prejudicial to, or unreasonable having consideration to the expectations of, the individual.

In particular, to the extent that these factors do require consideration of what is 'fair and reasonable' from the perspective of the individual, the APP entity should be required to consider and satisfy each factor. This is because the protection of personal information and right to privacy should be fundamental to the Act, and should not be readily outweighed by business considerations.

Proposal 10.3: ***Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.***

As a general position, the NSWCCL does not consider the use of personal information for purposes other than that for which it was collected is acceptable. However, the NSWCCL supports in-principle Proposal 10.3 as it appears to seek to minimise the risk of third-party collection, use or disclosure of personal information that has been unfairly or unlawfully collected, particularly where data may have been generated or inferred.

NSWCCL considers that adding a due diligence requirement ensures that APP entities do not simply assume that third party collection of personal information has complied with privacy requirements in the Act and the APPs is a necessary requirement. This is because it shifts the burden of privacy protection from individual users - who are not

well-equipped to self-manage opaque third party data collection - onto APP entities. This due diligence requirement would also support Proposal 10.1, creating an additional and appropriate safeguard for individuals.

Proposal 10.4: ***Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.***

The NSWCCL generally supports this amendment, as this strengthens the privacy protections for uses deemed to be a 'secondary purpose'. As suggested in **Proposals 10.1, 10.2**, and **10.3**, the proposed text should make clear that 'reasonably necessary' is to be adjudged by reference to the reasonable expectations of individuals and not the APP entity itself.

11. RESTRICTED AND PROHIBITED ACTS AND PRACTICES

Proposal 11.1:

Option 1 - APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- ***direct marketing, including online targeted advertising on a large scale;***
- ***the collection, use or disclosure of sensitive information on a large scale;***
- ***the collection, use or disclosure of children's personal information on a large scale;***
- ***the collection, use or disclosure of location data on a large scale;***
- ***the collection, use or disclosure of biometric or genetic data, including the use of facial recognition software;***
- ***the sale of personal information on a large scale;***
- ***the collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale;***
- ***the collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects; or***
- ***any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.***

Option 2 - In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice. Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

The Proposal

The NSWCCL supports the adoption of Option 1 above, but does not view the two options as mutually exclusive. The NSWCCL proposes that:

1. All specified restricted practices are added to the definition of sensitive information, requiring that an individual's consent is obtained prior to engaging in the restricted practice;

2. The Act be amended to allow for absolute opt-out rights in relation to restricted practices;

3. Proposals 16.1, 16.2, 16.3 and 16.4 be adopted in relation to ***all*** restricted practices (rather than only in respect of direct marketing), and;

4. Options 1 and 2 be combined to enable a best practice approach to privacy regulation in Australia.

Proposal 11.1 alone is insufficient protection against restricted practices

One of the principal problems with the current privacy regime is that there is an overreliance on consent and notification mechanisms. The best approach to privacy rights is not to engage in a 'box-ticking' exercise, whereby essential online services are locked behind a requirement to part with any control over an individual's personal information. Ultimately, organisations must be accountable for their activities in relation to privacy rights. Adopting restricted and prohibited practices ensures a risk-based approach to accountability in relation to privacy. This is consistent with the GDPR's '*scalable and proportionate approach to compliance*',[33] a model which ought to be adopted in Australia.

There are four broad comments that the NSWCCL makes in relation to Proposal 11:

- First, any amendments to the Act must reflect the practical reality that most people cannot self-manage all of their digital information, even if they are technologically sophisticated. The inability to self-manage data should not mean that you cede your privacy rights. Protections ought to be provided on the basis that privacy rights are human rights and should not be dependent upon the technological savvy of an individual. However, this does not mean that compliance mechanisms should be imposed on organisations and no control given to users of the data being collected. If privacy rights are to be respected then a mixture of both policy settings has to be implemented. There should not be a trade-off between an organisation's obligation to treat people's data responsibly, and the right of people to control how their data may be used. Both are essential, and complementary, tools to be employed in the privacy protection.

- Second, APP entities must be required to both implement measures to mitigate risks and be transparent about the way that information will be used to ensure that opt-in rights can be exercised in an informed manner. The fundamental issue with Option 2 is that it provides an 'all-or-nothing' circumstance: either provide all the personal information requested or do not use the service provided by the APP entity. That is an inappropriate way to deal with privacy rights and does not afford adequate protection. The mitigation of risks under Option 1 ought to expressly involve the minimisation of the collection of personal information. Alternatively, individuals should be empowered to be selective about the information provided to an APP entity, without the risk that key services will be unavailable.

- Third, we consider that most individuals would expect that APP entities collecting and using sensitive data will be aware of the risks that such collection and use may pose to the privacy of the consumer. Consequently, implementing such a requirement, we consider, would align with community expectations. The NSWCCL supports the introduction of requirements for APP entities to conduct Privacy Impact Assessments before commencing 'high risk' data projects. This would be in line with the requirements on government agencies under APP 1, and GDPR jurisdictions. Further, art 35(4) of the GDPR should be replicated in Australia; the OAIC should be required to publicise lists of restricted and prohibited practices to ensure that there is transparent collection of personal information.

- Fourth, by adopting elements from both Option 1 and Option 2, the Act can strike a balance between corporate accountability (by mandating restricted and prohibited practices) and providing individuals with the flexibility to exercise their privacy rights.

Specific Restricted Practices

[33] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk Based approach in Data Protection Legal Frameworks ' in 14/EN WP 218 (2014).

The Attorney-General has proposed specific provisions in relation to direct marketing, targeted advertising, and profiling in Chapter 16. The NSWCCL prefers a cohesive approach to restricted and prohibited practices. The best approach is to adopt the more rigorous standard taken in Chapter 16 and apply that to all restricted practices.

The NSWCCL otherwise agrees with the list of restricted practices contained in option one. The NSWCCL further agrees with the proposal that the OAIC could provide further clarity regarding the 'large scale' test.

Prohibited Practices

There are practices which should be prohibited and these should be outlined in the Act. The NSWCCL would support as good principle, the following No-Go Zones listed by the Office of the Privacy Commissioner of Canada.[34]

1. Collection, use or disclosure that is otherwise unlawful,

2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law,

3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual. 'Significant harm' includes bodily harm, damage to reputation and relationships, loss of employment and identity theft,

4. Publishing personal information online with the intended purpose of charging individuals for its removal,

5. Requiring passwords to social media accounts for the purposes of employee screening, and

6. Surveillance by an organization through audio or video functionality of the individual's own device.

12. PRO-PRIVACY DEFAULT SETTINGS

Proposal 12.1: ***Introduce pro-privacy defaults on a sectoral or other specified basis.***

- ***Option 1 – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.***

- ***Option 2 – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.***

The NSWCCL supports pro-privacy settings enabled by default (**Option 1**). The principle of privacy by default requires entities to ensure that personal information is handled with the highest privacy protections.

Recommendations by the ACCC in its *Digital Platforms Inquiry* report have already suggested that '*any settings for data practices relying on consent must be pre-selected to "off" and that different purposes of data collection,*

[34] Office of the Privacy Commissioner of Canada (May2018) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3), Inappropriate purposes or No-Go Zones <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>

use or disclosure must not be bundled'.[35] This is because the difference between an opt-in and an opt-out default can have a marked and significant effect on consumer participation.[36]

The NSWCCL also recognises that '*[n]o customer in a thousand ever read[s] the conditions*'.[37] Accordingly, because it is commonplace for consumers to not take the time to read the terms and conditions,[38] it is all the more important that pro-privacy settings are enabled by default so that consumers are protected by default given their otherwise vulnerable position. The NSWCCL's view is that opt-out regimes '*do not meet the requirement of consent as a freely given indication of the wishes of the data subject*'.[39] Instead, only an opt-in consent model can truly be viewed as 'real consent'.[40] If consent can only be achieved where freely given, in an informed manner, with current, specific and unambiguous and clear indications, then opt-out regimes clearly do not fall within this view of consent.

Moreover, as stated in relation to Proposal 9.1, it is clear that increasing the 'actionability' of privacy terms and conditions — in this case, requiring consumers to opt-out of the strong privacy protections (cf. opting in) — allows for better and more informed consent, further supporting the importance of having pro-privacy settings enabled by default

The NSWCCL considers that privacy should be ensured through organisational accountability, rather than individual action. This approach is consistent with international approaches, such as the GDPR. In this regard we note:

- The GDPR integrates accountability as one of its core principles. Article 5(2) of the GDPR states that '*[t]he controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ("accountability")*'.[41]

- The NSWCCL agrees with the submission by the Australian Privacy Foundation that consent requirements should state that 'the onus of proof of compliance with all consent conditions lies with the collector of the information'.[42]

- The NSWCCL considers that international harmony between privacy regulations is not only a desired goal but is also capable of guiding Australian privacy regulation in revealing where protection for Australian consumers is lacking.

[35] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 23 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

[36] Eric J Johnson, Steven Bellman and Gerald Lohse, 'Defaults, Framing and Privacy: Why Opting In-Opting Out' (2002) 13(1) *Marketing Letters* 5.

[37] *Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163, 169 (Lord Denning MR).

[38] Thus, resulting in low comprehension, a key element of informed consent according to Bashir et al: Masooda Bashir et al, 'Online Privacy and Informed Consent: The Dilemma of Information Asymmetry' (Conference Paper, American Society for Information Science, 6 November 2015) 43.

[39] Eleni Kosta, 'Construing the Meaning of "Opt-Out": An Analysis of the European, U.K. and German Data Protection Legislation' (Research Paper, Tilburg Institute for Law, 12 August 2015) 21.

[40] Ibid.

[41] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, art 5(2). See also: at recital 85.

[42] Australian Privacy Foundation, Submission to the Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (10 September 2019) 23.

13. CHILDREN AND VULNERABLE INDIVIDUALS

Proposal 13.1: ***Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:***

- ***Option 1 – Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.***
- ***Option 2 – In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.***

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

Overview

As set out above, privacy is a fundamental human right which is to be enjoyed by everyone – regardless of age, ability or status.[43] However, at present, the Act does not contain any specific protections for children or other vulnerable individuals, nor any general requirement for fair dealing with personal information.

The NSWCCL supports the notion of amendments to the Act that would provide protection of children's privacy in a more meaningful way. However, and consistent with the positions in respect of Notice and Consent (as set out above in sections 8 and 9 above), it considers there to be significant practical limitations and implementation issues with this proposal as currently framed. The fundamental problem to be addressed is the volume of data that is collected from children, which can be used for exploitative and harmful purposes. NSWCCL considers the Act should deal with online data 'from data creation and collection, through to its use, storage and processing, and its destruction (including the right to have personal information erased).[44]

Transparency and accountability are important, particularly where children's data is concerned. This is especially relevant in the context of online services, applications and social media platforms. Indeed, children need to be offered a necessary and discrete level of privacy that protects their privacy rights against undue interference, yet also respects their increasing ability to make their own privacy choices.[45]

This is because children are vulnerable due to limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making, particularly online. Children's ability to make rational decisions is further affected by cognitive biases.[46] This vulnerability is particularly relevant in the privacy context, due to the central role notice and consent have as the basis for current privacy protection.

As the current privacy protections relate to children, it is clear that the frameworks regarding consent and notice were designed pre-internet, when social media platforms were yet to be invented. Indeed, despite the profound

---

[43] *Universal Declaration of Human Rights*, Art 12; *International Covenant on Civil and Political Rights*, Art 17.

[44] UNICEF, UNICEF Guidelines for Industry on Child Online Protection (2015), accessible at <https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf>

[45] References to 'Child' or 'Children' are understood to mean anyone under the age of 18 years of age. This is in accordance with the State and Territories Age of Majority legislation, and the United Nations Convention on the Rights of the Child (UNCRC), which defines a child as everyone under 18, "*unless the law applicable to the child, majority is attained earlier*." Australia ratified this convention in December 1990, meaning it has a duty to ensure that all children in Australia enjoy the rights set out in the treaty.

[46] See, Sonia Livingstone, Mariya Stoilova and Rishita Nandari, '*Children's data and privacy online – Growing up in a digital age: An evidence review*' (London School of Economics Media and Communications, December 2018 < https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf>, p. 17.

benefits of the internet, children in particular can be faced with a number of risks, including exposure to inappropriate content for their age and inappropriate contact. They also face risk related to online privacy in terms of data collection and usage and the collection of location information.[47]

Accordingly, the NSWCCL considers that much of the data collection behaviour directed at children should be by way of 'No Go Zones'.[48] Legislation enshrining 'No Go Zones' specific to children would offer a base-level of protection, regardless of consent, by identifying and prohibiting collection, use, and disclosure practices that are generally considered inappropriate based on the known vulnerabilities associated with children. One example is a prohibition on the collection of information for use in targeted online advertising to children.

Moreover, the NSWCCL notes that a key issue, which any proposed amendments to the Act should address, is the exploitative and harmful amount of data that is collected. Accordingly, it is of the view that any amendments to the Act should expressly deal with the online data of children '*from data creation and collection, through its use, storage, and process, to its destruction'.* In addition, and as addressed in further detail in the response to Proposal 14 below, this should also include a right to have personal data erased.[49]

Should APP entities be permitted to assess capacity on an individualised basis in circumstances where it is practical to do so?

The NSWCCL does not support the notion that APP entities be permitted to assess the capacity of a child on an individualised basis, either in circumstances where it is practical to do so or otherwise.[50]

Whilst the capacity of an individual (including a child) must generally be determined on the basis of individualised assessment,[51] the assessment of capacity for each individual child whose data an APP entity wishes to handle creates significant practical implementation issues. Essentially, this would require an unidentified decision-maker (or potentially an algorithm in the case of an online platform) to correctly assess whether a child has sufficient capacity to consent.

If APP entities were to assess on an individualised basis whether a child has the capacity to consent to privacy notices and requests, this would require, at a minimum, an assessment of whether they have '*sufficient understanding and maturity to understand what is being proposed.*'[52] This is largely a subjective evaluation on the part of a decision-maker – and is one that could potentially create further risk for a child if there is, for example, a failure to correctly identify any lack of capacity. Indeed, it would be counterproductive if a requirement to assess a

[47] See, in particular, UNICEP Guidelines for Industry on Child Protection (2015), p. 7 < https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf>

[48] See for example, in the Discussion Paper published by the Office of the Privacy Commissioner of Canada, "No Go Zones" were proposed as, in effect, a prohibition on collection, use or disclosure of personal information in certain circumstances – irrespective of consent.

[49] See, in particular, UNICEP Guidelines for Industry on Child Protection (2015) < https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf>

[50] It is noted that item B.58 of the Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (22 July 2019), provides further guidance regarding an APP entities' ability, in circumstances where it is not practicable or reasonable, to make certain presumptions regarding an individual's age and capacity to consent. Item B.58 is also not supported.

[51] See, Norman Witzleb, Moira Paterson, Jordan Wilson-Otto, Gabby Tolkin-Rosen and Melanie Marks, 'Privacy risks and harms for children and other vulnerable groups in the online environment' (Research Paper, Office of the Australian Information Commissioner, 18 December 2020) https://www.oaic.gov.au/_data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf, page 83. With respect to children, the case-by-case model for assessing capacity would also be consistent with the approach taken in the UNCRC. See Article 12(1), which requires all states to "*assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child*".

[52] See Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (22 July 2019), Children and young people, item B.57.

child's capacity creates additional privacy risks – especially if those risks outweigh the privacy concerns the proposal seeks to address.

Further, whilst the current proposal only contemplates potentially permitting APP entities to assess the capacity of a child on an individual basis in circumstances '*where it is practicable to do so*', this may nonetheless leave open the possibility that, in circumstances where it is *not* practicable or reasonable for the APP entity to assess a child's capacity, it may otherwise rely on certain presumptions regarding a child's age and/or capacity to consent.[53] Such an approach is inherently risky for the protection of children's rights, and calls into question exactly how an APP entity is to practically assess children's capacity on an individualised basis.

Circumstances in which parent or guardian consent must be obtained

As noted above, at present the Act seeks to protect an individual's personal information regardless of their age. It does not, however, specify an age after which an individual can make their own privacy decisions.

Consistent with the position regarding the Consent and Notice models more generally, the NSWCCL considers there to be the related implementation issues with using parental or guardian consent for children – particularly in an online environment. This is for a number of reasons, including:

- First, the provision of consent by a parent or guardian on behalf of a child is based on the assumption that parents and guardians are better able to assess the consequences of providing consent than a child. In an online context, if a parent or guardian does not read or fully understand the privacy policy, or there is no real choice but to accept in order to use the service, then it makes no differences to the protection whether it is the parent or child who has provided the requested consent.

- Second, there is a further risk that a parent or guardian similarly lacks the required digital literacy in relation to applications and services used by children to know what consent is truly being provided for.

- Third, an additional problem with relying on parental or guardian consent relates to effectiveness. There are numerous examples whereby children can easily circumvent age restrictions or consent requirements to gain access to services and applications they wish to join, rendering the consent barriers redundant.

It follows that a framework that relies heavily on parental or guardian consent cannot fully address some fundamental problems, which include the digital divide between parents and children and the general weakness of the Notice and Consent models. The NSWCCL considers that reliance solely on parental or guardian consent mechanisms is a problematic way of protecting the privacy of children, particularly online.

The NSWCCL is of the view that these problems may potentially be reduced in models that rely more heavily on accountability of the APP entity, make particularly problematic privacy invasive practices '*No Go Zones*' or require justification on grounds other than parental or guardian consent.

Ultimately, any amendments to the Act regarding capacity and consent should properly reflect the difficulty of obtaining meaningful consent to such data practices from children, and in particular, in circumstances where they may not understand the associated privacy consequences. Moreover, if some kind of alternative age limit to verification is proposed (such as facial recognition or biometrics, rather than simply entering a birthdate that meets the requested age criteria), this may create digital identification privacy concern, not just for children, but for all digital online users.[54]

[53] See Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (22 July 2019), Children and young people, item B.58.

[54] See, for example, Cam Wilson, *'Online age verification: what is it and why are people really worried about it?'* Crikey, 9 November 2021 < https://www.crikey.com.au/2021/11/09/online-age-verification-what-is-it/?>

Proposal 13.2: ***Require APP 5 notices to be clear, current and understandable, in particular for any information addressed specifically to a child.***

The NSWCCL supports a proposal that would require APP 5 notices to be clear, current and understandable, and in particular '*for any information addressed specifically to a child*'. The NSWCCL also considers that the provision of APP 5 notices should continue to be made in a timely manner.[55]

However, further explanation and consultation regarding the practical application of this proposal in terms of how any information is to be specifically addressed to children, and the form it is to be provided in, is required.

The NSWCCL notes that, at present, APP 5 requires an APP entity that collects personal information about an individual to '*take reasonable steps*' either to notify the individual of certain matters or to ensure the individual is aware of those matters.[56] The onus therefore lies with the APP entity to show that the steps taken are reasonable given the knowledge and awareness of the individual. Moreover, whilst APP 5 does not deal specifically with children, the APP Guidelines do note that '*any special needs of the individual*' should be taken into account in determining what steps are reasonable.

Accordingly, in view of the vulnerability and need for distinct protections for the special needs of children, the NSWCCL supports a proposal that APP 5 notices, and in particular those provided by APP entities whose services are targeted to or used by children, should take particular care in designing effective privacy notices for children.

Likewise, this should include factors such as taking steps to ensure that, amongst other things, the content of the notification is tailored in terms of content, style, mode of delivery and timing to be effective and appropriate for the variety of ages and abilities of individuals whose information will be collected (i.e., plain and clear language that a child could understand).[57]

14. RIGHT TO OBJECT AND PORTABILITY

Proposal 14.1: ***An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using, disclosing the individual's personal information and must inform the individual of the consequences of the objection.***

The NSWCCL generally supports the proposal that an individual may object or withdraw their consent to the collection, use, or disclosure of their personal information. However, having regard to the way that analogous provisions work internationally, particularly in GDPR jurisdictions, the NSWCCL would equally support the adoption of a stronger regime to protect the right to object.

The NSWCCL considers there to be two short points in this regard, which should be taken into account in the drafting of any proposed amendments to the Act:

- First, in contrast to the analogous provisions in the GDPR, the proposal does not provide for a time-frame for compliance. This is an important procedural step that the NSWCCL thinks should be included so as to ensure practical compliance by responsible entities.[58]

[55] See, *Privacy Act 1988* (Cth), Schedule 1, Australian Privacy Principle 5 – Notification of the collection of personal information, s 5.1.

[56] *Privacy Act 1988* (Cth), Schedule 1, Australian Privacy Principle 5 – Notification of the collection of personal information, s 5.1, which provides that "*[A]n APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances*".

[57] See, e.g., Lego Group Privacy Policy (last modified 20 June 2018) < https://www.lego.com/en-au/legal/notices-and-policies/privacy-policy/>.

[58] See, GDPR, Article 21.

- Second, the use of the words '*reasonable steps*' ought to be considered in light of the ease with which consumers can withdraw their consent or object to the use of their personal information. The GDPR provides that the withdrawal of consent must be as easy as the provision of consent.

15. RIGHT TO ERASURE OF PERSONAL INFORMATION

Proposal 15.1: ***An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:***

- ***the personal information must be destroyed or de-identified under APP 11.2;***
- ***the personal information is sensitive information;***
- ***an individual has successfully objected to personal information handling through the right to object (see Chapter 14);***
- ***the personal information has been collected, used or disclosed unlawfully;***
- ***the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information; and***
- ***the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.***

Proposal 15.2: ***Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.***

Overview

The right to erasure is an important and controversial matter, with many considerations and choices in a policy setting to be made. Indeed, in the digital era there is clearly a growing concern about the ability for individuals to protect and control the dissemination of their personal data – particularly online.

The NSWCCL generally supports the proposal for a right to erasure, and is of the view that such a right should not be met with any immediate barriers. Notwithstanding, the NSWCCL agrees that such a right should not be absolute in application – rather, certain qualifications by exceptions should apply (as contemplated by Proposal 15.2). Indeed, the NSWCCL recognises that, in practical terms, certain discretions or scope may be required for certain situations where data should not be erased, such as those related or linked to certain government and national security or health services.

Such qualifications and exceptions are seen as required in order to balance the competing interests of APP entities, the broader public, legal requirements, and, importantly, an individual's privacy interests. Accordingly, the NSWCCL supports the proposal that the Act be amended so that, subject to exceptions, individuals can make a request for erasure of personal information where one of the six identified grounds applies.[59]

The NSWCCL otherwise considers that further consideration, development, and consultation is required regarding the practicalities of the application of these exceptions and an individual's right to make such request. It considers that this may potentially include consultation on whether, for example, it is necessary to ensure that the relevant Court or Tribunal that may hear such requests has the necessary jurisdiction (as an independent cause of action, rather than the as a consequence of another action) to order the destruction of personal information.

[59] The NSWCCL considers that amendments requiring a request for erasure to be made only where the six identified grounds apply is also largely consistent, and would bring the Australian Privacy laws in-line with other overseas jurisdictions; see for example, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 17.

Feedback on what exceptions may be appropriate for a right to erasure in the Act to address concerns in relation to freedom of speech, challenges during law enforcement and national security investigations, and practical difficulties for industry

The NSWCCL agrees with the submissions that any potential exception to a right to erasure of personal information needs to find a balance between the competing interests of privacy and exercises of freedom of speech or expression, law enforcement, national security, and practical difficulties for industry. Proposals for modelling such exceptions on the public interest test set out in the *Freedom of Information Act* 1982 (Cth)[60] would, seemingly, go towards achieving such balance.

Further, the NSWCCL supports the proposal for the development of further guidance on determining what is in the public interest and what could include erasure or retention of personal information. The NSWCCL otherwise considers that careful attention should be given to the development of case law as it relates to the public interest test, so that some further clarification may be identified in respect of the circumstances which would be in the public interest to support rejection of an erasure request.

How APP entities should determine whether one of the exceptions applies in practice

The NSWCCL understands that the proposal of a right to erasure is intended to complement the existing rights under the Act. For example, APP entities already have an existing obligation under APP 11.2 to destroy or de-identify personal information when it is no longer necessary for any purpose for which it may be used or disclosed under the APPs.

Related to this, the NSWCCL acknowledges the concerns about the introduction of a right to erasure potentially creating more onerous obligations for APP entities. However, it is noted that entities should already, presumably, have practices, procedures and systems in place to give effect to the requirements of APP 11.2. As such, the addition of a right to erasure merely extends this obligation, so as to enable individuals to initiate this process on request.

Indeed, in terms of the practicalities of the introduction of a right to erasure, the NSWCCL would support the development of further guidance or a checklist to assist APP entities in determining whether one of the exceptions applies.[61] It considers, however, that emphasis should be given to the fact that the exceptions do not all apply in the same way, and so an APP entity will be required to examine each exception on a case-by-case basis. The NSWCCL provides further related comments regarding this matter in response to proposal 15.3 below.

Would the proposed public interest exception appropriately protect freedom of speech?

The NSWCCL recognises that, in certain circumstances, there may be public interest reasons to reject a request for erasure of person information, including for reasons such as freedom of speech or expression. Indeed, the need to find a balance between a right to erasure and to protect freedom of speech is crucial in achieving greater clarity and effective application in Australian privacy law.

However, it should be noted that whilst certain overseas data protection laws typically contain exceptions for legally enshrined rights such as freedom of expression and freedom of information, any exception ultimately needs to reconcile the competing interests of privacy, freedom of expression and the retention of information in the public domain on a case-by-case basis. Accordingly, the NSWCCL is of the view that the development of any precedent relating to this right should be left to the relevant Court or Tribunal considering such matters as they arise, and the drafting of any amendments to the Act should be mindful of not attempting to pre-emptively legislate in this regard.

Should a right to erasure apply to personal information available online, including search results?

[60] See, *Freedom of Information Act 1982* (Cth), sections 11A(5) and 11B(3).

[61] See, in particular, UK Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR), Checklist and guidance on the application of Exemptions, (1 January 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>

The NSWCCL recognises that the need for the protection of personal information and privacy in the internet era is a complex issue and involves considerations of the intersection of technology and the law which demand a flexible and innovative approach.

However, the NSWCCL considers there are significant practical limitations for a right to erasure applying to all personal information available online, including search results.

The NSWCCL is of the view that a potential right to erasure should be applicable to all data controllers, however, the processing of personal information carried out in the context of the activity of a search engine provider (i.e., Google, Yahoo!, or Bing) must be distinguished from processing that is carried out by publishers of third-party websites, such as media outlets that provide online newspaper content.

Ultimately, this is because, even if a search engine provider removes a link, they cannot delete the information from the webpage that it is published on, or take down the webpage from the internet. Any such requests for the erasure of personal information would need to be made directly to the website in question (and then be subject to any potential exceptions, as set out above).

All the same, and consistent with the GDPR protections, to the extent that the construction of a search index involves a collection of personal information which is no longer necessary in relation to the purposes of the processing by the search engine, the NSWCCL would support the extension of the right to erasure to the de-indexing of search results on search engines.

Proposal 15.3: ***An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.***

Further to the matters set out above regarding APP entities' determination of whether an exception applies, the NSWCCL considers that any response to an erasure request should be within a reasonable period. Consistent with the UK GDPR,[62] any such response should be made without undue delay, and within at least one month from the receipt of the request, with the time limit commencing upon the receipt of the request.

The NSWCCL also considers that it may be necessary to adopt some requirement that a party may, in certain circumstances, extend the period of time to respond (by a set period). Such circumstances may include if the request is particularly complex, or if multiple requests may have been received from the same individual.[63]

Moreover, the APP entity in question should be required to provide notification to the individual of whether the entity has in fact erased the data the subject of the request or, in the event that the request has been refused, the basis of the refusal. Further consideration and guidance should also be provided in terms the avenues for relief in the event that an APP entity fails to respond within a reasonable period, or if an individual wishes to appeal the refusal of a request.

16. DIRECT MARKETING, TARGETED ADVERTISING AND PROFILING

Proposal 16.1: ***The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object***

[62] UK Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR) – Individual Rights: Right to erasure", (1 January 2021) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#top>

[63] UK Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR) – Individual Rights: Right to erasure", (1 January 2021) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#top>

in relation to each marketing product provided. On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

Proposal 16.2: ***The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.***

Proposal 16.3: ***APP entities would be required to include the following additional information in their privacy policy:***

- ***whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual; and***
- ***whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.***

Proposal 16.4: ***Repeal APP 7 in light of existing protections in the Act and other proposals for reform.***

The NSWCCL has addressed these proposals in the response to Proposal 11.1 above. The NSWCCL considers that there should not be an arbitrary distinction drawn between direct marketing, targeted advertising and profiling, and the restricted practices outlined in Chapter 11 of the Discussion Paper.

17. AUTOMATED DECISION-MAKING

Proposal 17.1: ***Require privacy policies to include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant effect on people's rights.***

The NSWCCL considers that Proposal 17.1 does not go far enough to protect individuals from the deleterious effects of automatic decision-making (**ADM**) that has a legal or similarly significant effect on an individual's rights. The NSWCCL supports the introduction of a prohibition on ADM that has legal or similarly significant effects, subject to limited exceptions similar to the prohibition contained in GDPR Article 22. Merely requiring entities to provide notice of ADM that has legal or similarly significant effects does not go far enough to protect individuals from algorithmic decision-making.

Strong protections against the use of ADM are necessary because this form of decision-making is opaque and secretive, making it very difficult for individuals to identify and challenge automated decisions. The NSWCCL considers that increasing reliance on ADM by entities carries the risk of cloaking and amplifying discrimination. For one, ADM is difficult for individuals (and even entities) to understand, due to the opacity, complexity and unpredictability of algorithms. Further, ADM is liable to entrench inequality because it relies on datasets that reflect persistent and widespread societal biases, disadvantaging historically undersampled minorities. A cautionary tale in this regard is the Commonwealth Government's 'Robodebt' debacle. ADM processes were relied upon to identify potential welfare fraudsters. The calibration of the ADM process and the lack of transparency regarding the criteria to assess the legitimacy of the claims led to a series of poor outcomes for already marginalised groups.

ADM systems may also heighten the risk that individuals will be subject to unfair or unlawful discrimination. Shaun Chung and Rohan Shukla referred to the potential for predictive policing to '*reinforce historical racial bias and enable targeted policing of a specific demographic*'.[64]

[64] Stan Cheung and Rohan Shukla, *Submission to the Privacy Act Review* (November 2020), 7.

NSWCCL submits that from a privacy and data protection perspective, ethical and responsible ADM should be the a policy objective of law makers. In this regard, we consider further oversight by an independent body of ADM processes is required (noting OAIC may be best placed to perform this role, provided it has the adequate resources).

Other Jurisdictions

NSWCCL suggests that further guidance with respect to this proposal may be gleaned from other jurisdictions. For example:

- The GDPR requires that individuals be given prior notice of the use of personal data in ADM, including profiling. The GDPR also provides a right to access information about the existence of ADM and '*meaningful information about the logic involved, as well as the significance and the envisaged consequences*' of such processing to the individual. The GDPR contains a prohibition against 'decisions based solely on automated processing' which has legal or similarly significant effects (e.g. decisions about credit, or employment) and requires controllers to implement measures to enable individuals to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

- In California, the CPRA will allow regulations to be developed to grant access and opt-out rights with respect to ADM technology, and will require businesses' responses to access requests to include meaningful information about the logic involved in such decision-making processes.

The NSWCCL Position

The NSWCCL considers that in cases where ADM occurs, entities should implement suitable measures to safeguard the rights and interests of individuals, including by providing the right to obtain meaningful human intervention and the ability to contest the decision. The NSWCCL considers that the following requirements for ADM should be introduced into the Act:

- Individuals should receive prior notice that an entity uses ADM systems. The AHRC report recommended that government and private sector entities be required to notify of the use of AI in decision making where it is materially used in making an administrative decision, or where it has a legal, or similarly significant effect on people's rights, respectively. This would bring Australian in line with the GDPR

- In light of the potential harm to individuals from decisions made by ADM systems that rely on their personal information, APP entities could be required to state in privacy policies whether an entity will use personal information for ADM. This would increase transparency about when their personal information is used in ADM that affects them.

- Individuals should have a defined right to opt-out of ADM, and have an easy and accessible complaints and review process. Importantly, individuals ought to be given the right to have these decisions reviewed by a human decision-maker. This is consistent with the GDPR and the CPRA in California, which reflect best practice in relation to ADM and privacy rights.

18. ACCESSING AND CORRECTING PERSONAL INFORMATION

Proposal 18.1: ***An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.***

Proposal 18.2: ***Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:***

- ***the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.***

Proposal 18.3: ***Clarify the existing access request process in APP 12 to the effect that:***

- ***an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature; and***

- ***where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.***

The NSWCCL generally supports greater transparency on the part of APP entities and greater ability for individuals to access and correct their personal information.

Given that the NSWCCL agrees that inferred information should be included in the definition of 'collects', it makes sense for organisations, upon request, to be required to identify the source of personal information where that information has been collected indirectly. The NSWCCL supports **Proposal 18.1** along with the qualification of 'impossible or would involve disproportionate effort'. However, the Act should clarify both standards of 'impossible' and 'disproportionate effort' to provide some guidance in order to ensure that entities do not overuse the exception.

Regarding the notion of impossibility, this should be a high bar – there are few situations that would fall within this exception. Guidance from the UK Information Commissioner's Office (**ICO**) suggests that where this occurs, the entity should nevertheless publish the relevant privacy information about its activities, such as on its website.[65]

Regarding 'disproportionate effort', guidance from the ICO has indicated that an entity must be able to show that the effort involved in providing the information is not warranted by the impact on the data subject.[66] Suggested factors for consideration are as follows:

- the more significant the effect on the individual, the less likely it is that the entity can rely on the exception;
- the fewer the number of individuals involved, the less likely it is that the entity can rely on the exception;
- the newer the personal data involved, the less likely it is that the entity can rely on the exception;
- where the entity has not implemented appropriate safeguards, the less likely it is that the entity can rely on the exception; and

[65] UK Information Commissioner's Office, 'Are there any exceptions?', *ICO* (Web Page) < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/>.
[66] Ibid.

- where the entity relies on the exception, it should still publish privacy information (e.g., on its website) stating that certain kinds of information will be used – this can potentially be in line with privacy policy requirements.

The NSWCCL supports **Proposal 18.2** and the balancing of privacy protections against natural justice processes. However, we suggest that limitations are placed on this, including the following:

- the dispute resolution process must either be imminent or ongoing, instead of being a mere possibility; and

- once the dispute resolution process is agreed to be concluded and the individual still requests access to the personal information, the entity should no longer be allowed to rely on the dispute resolution exception.

The NSWCCL supports the provision of information in a human-interpretable manner that makes sense to the requesting individual. This is particularly important as expanding the definitions of 'personal information' and 'collects' is likely to bring in large amounts of technical information that are difficult to process and understand. In order for access to be meaningful, individuals must be able to understand what they are given access to.

Accordingly, the NSWCCL supports the amendments suggested in **Proposal 18.3** to allow an APP entity to consult with the individual for alternative provisions of the requested information in a manner, noting that what is agreed upon must meet the needs of both parties and should not be a way for the APP entity to sidestep data access requirements.

The NSWCCL also supports the requirement for an APP entity to provide an explanation of the personal information where it is not readily understandable to an ordinary reader. This allows data access to be given effect in practice, as the notion of understandability is arguably inseparable from meaningful data access and correction – if the individual is unable to understand the data that is accessed, then the data cannot be corrected. In New Zealand, the Privacy Commissioner guidelines state that it is reasonable for individuals to ask that the information is given to them in an understandable form.

19. SECURITY AND DESTRUCTION OF PERSONAL INFORMATION

Proposal 19.1: ***Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.***

Proposal 19.2: ***Include a list of factors that indicate what reasonable steps may be required.***

Proposal 19.3: ***Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.***

The NSWCCL supports the amendment of APP 11.1 to clarify the 'reasonable steps' entities are required to take to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure. The NSWCCL considers that clearer security requirements, including a list of factors that indicate what reasonable steps may be required (**Proposal 19.2**), will increase protections for individuals from data breaches.

The NSWCCL also supports the introduction of a requirement for APP entities to take 'all reasonable steps' to destroy or anonymise information where the APP entity no longer needs the information for use or disclosure (**Proposal 19.3**). This would provide greater privacy protection, as the current wording of 'such steps as are reasonable in the circumstances' is overly permissive in allowing APP entities to be less rigorous in applying privacy protections to the information. There is, consequently, the risk that data is either kept for longer than it should be or is not destroyed completely but may still be accessible.

20. ORGANISATIONAL ACCOUNTABILITY

Proposal 20.1: ***Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:***

- ***amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.***

The NSWCCL strongly agrees with the introduction of further organisational accountability requirements into the Act. In light of information and power asymmetries in the processing of personal information, individuals should not be expected to bear the burden of managing privacy risks themselves. Accordingly, it is incumbent on organisations to introduce accountability measures, including clear records of the purposes for which personal information is used.

Organisational accountability requires entities to implement different actions and controls to comply, and demonstrate compliance, with the privacy regulatory framework. This includes data protection and privacy requirements being embedded into internal processes and procedures, such as through record keeping requirements.

Placing the burden of privacy protection onto the individual is unfair and impractical. It is the organisations that hold personal information – governments and businesses – that must bear responsibility for respecting the right to privacy. The NSWCCL considers that while individuals should be given the tools and knowledge to meaningfully engage in privacy self-management, this should be complemented by organisational accountability measures to ensure that the burden of understanding and consenting to complicated practices does not fall solely on individuals.

Accordingly, the NSWCCL supports the amendment of APP 6 to expressly require APP entities to determine, upon or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes. Such records are necessary for individuals to assert their data rights (including e.g. the right to object and the right to erasure), and to embed privacy considerations into organisational culture.

The NSWCCL strongly supports APP entities, before or at the time of obtaining information, recording the secondary purposes for which the information was sought. We note that this is more important in areas where there are greater privacy risks.

Part Three: Regulation and Enforcement

24. ENFORCEMENT

Proposal 24.1: ***Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:***

- ***a new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy;***
- ***a series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.***

NSWCCL supports the creation of a new mid-tier civil penalty provision for any interference with privacy. However, it does not support the creation of a tier of civil penalty provisions that respond to low level and clearly defined breaches of certain APPs.

A number of domestic jurisdictions have introduced tiered civil penalty regimes. For example, the *Statutes Amendment (National Energy Laws) (Penalties and Enforcement) Act 2020* (SA) introduced a tiered civil penalty regime under the National Electricity Law (**NEL**) and the National Gas Law (**NGL**) applied in most Australian states.[67] Regimes under both the NEL and NGL contain three tiers of penalty provisions, with each tier differentiated by the severity of the contravention. The NSWCCL considers that implementing a similar regime would allow the OAIC to better respond to breaches as it gives the OAIC a greater range of enforcement tools and bridges the gap between an IC-issued determination and the higher civil penalty for serious or repeated interferences.

The NSWCCL considers the cost and time burden on the OAIC in enforcing low level breaches to be too great when considering that the provisions only address administrative breaches without the need for establishing actual harm. The notion that the OAIC should only issue such infringement notices where they are prepared to pursue the matter in court in the event of non-payment is also at odds with the purported purpose of this infringement notice regime, which is to simply address administrative breaches which otherwise would not have necessitated legal proceedings.

Proposal 24.3: ***The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.***

The NSWCCL supports the broadening of the OAIC's investigation powers in order to assist its fact-finding functions. However, the NSWCCL submits that the broadening of OAIC's investigation powers must be accompanied with adequate resourcing for OAIC, and that OAIC must be consulted in this regard.

Proposal 24.4: ***Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.***

[67] The National Electricity Law (NEL) and National Gas Law (NGL) are contained as schedules to the *National Electricity (South Australia) Act 1996* (SA) and *National Gas (South Australia) Act 2008* (SA) respectively. South Australia is the lead legislator in regards to energy legislation. Each of these are applied as law in each participating jurisdiction through application statutes. Most jurisdictions have implemented such statutes.

NSWCCL supports amending the Act to empower the IC to undertake public inquiries and reviews into specified matters. It considers it important that such a power be unfettered and be self-referrable.

Public inquiries and reviews conducted by other agencies are not uncommon and have enjoyed recent success. For example, the ACCC's Digital Platforms Inquiry resulted in acceptance by the Commonwealth government that there was a need to promote competition, enhance consumer protection and support a sustainable Australian media landscape in the digital age.[68] The government has undertaken a number of actions following this inquiry including the development of a digital platforms specialist branch at the ACCC,[69] a broad review of Australian privacy law,[70] and the development and enactment of a News Media Bargaining Code.[71]

Proposal 24.5: ***Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:***

- ***a declaration that the respondent must perform any reasonable act or course of conduct to <u>identify, mitigate</u> and <u>redress any actual or reasonably foreseeable</u> loss or damage suffered by the complainant/those individuals.***

The NSWCCL supports the amendments to paragraph 52(1)(b)(ii) and 52(1A)(c) to require APP entities to identify, mitigate and redress actual or reasonably foreseeable loss on the basis that they should be liable for the foreseeable consequences of their actions.

In implementing this proposal, NSWCCL considers it important that 'reasonably foreseeable loss or damage' is defined to ensure that both the OAIC and APP entities are clear as to the operation of the provision. The NSWCCL advocates for the term to take on a definition that is similar to that in negligence—that is, whether the loss or damage is reasonably foreseeable by a a reasonable person in the APP entity's position and the loss is not far-fetched or fanciful.[72]

Proposal 24.6: ***Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.***

The NSWCCL supports the conferral of power on the Federal Court to make any order it sees fit after a section 13G civil penalty provision has been established on the basis that it reduces caseloads and streamlines the complaint process.

[68] See Australian Government, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Government Response, 12 December 2019) 3 <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf>

[69] See Australian Competition and Consumer Commission, Digital Platforms <https://www.accc.gov.au/focus-areas/digital-platforms>.

[70] See Attorney-General's Department, Review of the Privacy Act 1988 <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

[71] *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act* (Cth); Australian Competition and Consumer Commission, News media bargaining code <https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code>.

[72] *Wyong Shire Council v Shirt* (1980) 146 CLR 40, 47 (Mason J) affirmed in *New South Wales v Fahy* (2007) 232 CLR 486, 491 [7] (Gleeson CJ), 504 [56] (Gummow and Hayne JJ), 523 [118] (Kirby J), 550 [213] (Callinan and Heydon JJ).

Proposal 24.7: ***Introduce an industry funding model similar to ASIC's incorporating two different levies:***

- ***a cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and***
- ***a statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.***

The NSWCCL supports the introduction of an industry funding model similar to ASIC's incorporating a cost recovery levy and a statutory levy.

Regarding the cost recovery levy, the NSWCCL considers that the OAIC should be able to recover from businesses the costs incurred in providing guidance, assistance and advice to organisations in the form of a fee schedule for the type of assistance requested. Regarding the statutory levy, the NSWCCL considers that health service providers and the finance industry should bear a part of the OAIC's costs of investigating complaints and undertaking enforcement action in courts. This is because these industries have consistently notified the largest amount of data breaches in the past two years,[73] indicating the high privacy risks in these industries. It may also be appropriate for the legal, accounting and management services industry, education providers and the insurance industry to bear a portion of the cost as these industries have also notified significant data breaches in the past two years.[74]

Proposal 24.8: ***Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.***

NSWCCL supports amending the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged, including numbers dismissed under each ground.

The release of information increases accountability and improves the quality of the OAIC's decision making in regard to their complaint handling process. Apart from Senate estimates, annual reports are often the only way complainants can get relevant information about the operation of the Act.

Proposal 24.9: ***Alternative regulatory models***

- ***Option 1 – Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.***
- ***Option 2 – Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.***
- ***Option 3 – Establish a Deputy Information Commissioner – Enforcement within the OAIC.***

The NSWCCL supports the third option to establish a Deputy Information Commissioner – Enforcement within the OAIC.

[73] See OAIC, Notifiable Data Breaches Report: July – December 2019; OAIC, Notifiable Data Breaches Report: January-June 2020; OAIC, Notifiable Data Breaches Report: July –December 2020; OAIC, Notifiable Data Breaches Report: January-June 2021.

[74] See OAIC, Notifiable Data Breaches Report: July – December 2019; OAIC, Notifiable Data Breaches Report: January-June 2020; OAIC, Notifiable Data Breaches Report: July –December 2020; OAIC, Notifiable Data Breaches Report: January-June 2021.

The NSWCCL is of the view that the OAIC should retain both its conciliation and enforcement functions, albeit in a more structured manner with the introduction of a specific sub-division. NSWCCL considers this structure to be the best of the three options because: (1) it reduces the need to share information across different agencies; (2) it provides the OAIC with visibility over emerging issues within this space as a result of its heightened exposure to privacy issues; and (3) it eliminates the need to reduce the OAIC's funding to fund a new agency.

25. A DIRECT RIGHT OF ACTION

Proposal 25.1: ***Create a direct right of action with the following design elements:***

- ***the action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity;***
- ***the action would be heard by the Federal Court or the Federal Circuit Court;***
- ***the claimant would first need to make a complaint to the OAIC (or FPO)1 and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman;***
- ***the complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application;***
- ***the OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.***

The NSWCCL supports the creation of a direct right of action.

The NSWCCL considers it important that individuals can personally litigate a claim for breach of their privacy under the Privacy Act. However, the ability of individuals to do so is currently limited.[75] The creation of a direct right of action would therefore give individuals greater control over their personal information by providing an additional avenue of redress under the Privacy Act.[76] This, in turn, would encourage better compliance by APP entities of their privacy obligations under the Act.[77]

The NSWCCL generally agrees with the proposed model, but considers it important that the following modifications are made in order to strike the correct balance.

Small claims procedure

A 'small claims procedure' modelled on existing 'small claims' regimes should be created for minor privacy matters. The principal justification for this is based upon the belief that traditional courts have proven to be too costly, unduly technical, tortuously prolonged and overly formal, especially in relation to small claims.[78]

In Australia, the Commonwealth and individual States have each developed their own responses to the problems associated with the increasingly prohibitive costs of justice and the unsuitability of the common law and its formal adversarial mechanisms to handle disputes involving small claims.[79]

---

[75] Angela Potter et al, *Comparing privacy laws: GDPR v. Australian Privacy* Act (Report, 26 March 2020) <https://www.dataguidance.com/sites/default/files/gdpr_v_australia.pdf>

[76] Ibid.

[77] Ibid.

[78] E Eugene Clark, 'Small Claims Courts and Tribunals in Australia: Development and Emerging Issues' (1991) 10(3) University of Tasmania Law Review 201 <http://www.austlii.edu.au/au/journals/UTasLawRw/1991/7.pdf>.

[79] Ibid.

At the Commonwealth level, the Federal Circuit Court rules limits the small claims procedure to employment issues under the Fair Work Act.[80] Therefore, to apply this to breaches of privacy, the jurisdictional scope of this regime would need to be expanded to cover privacy disputes.

Alternative to the OAIC

The claimant should not need to first make a complaint to the OAIC on the basis given this would increase the burden on the agency (whereas the purpose of this proposal is to reduce it). Instead, a court-sponsored ADR process before hearings could be more favourable process for complainants.

Judicial proceedings in the Federal Courts require ADR to be attempted before making an application as a case management strategy[81] in an effort to reduce backlogs of cases and enable the cheaper resolution of disputes.[82] Given the success of such processes, NSWCCL submits that this process would provide a more efficient and effective alternative to going through the OAIC[83] and that complainants thus should be able to go through the court process immediately.

Leave of the court

There should be no need to seek leave of the court to make the necessary application.

Harm threshold

For a direct right of action, there is a need to balance giving individuals greater control over their information and incentivising organisational compliance against the need to ensure court resources are appropriately directed.[84] While a harm threshold is necessary, the NSWCCL considers that it should be lower than being limited to only 'serious' breaches of privacy as it could preclude many individuals from seeking recourse.[85]

For this reason, and for the sake of consistency between OAIC and individual actions, the NSWCCL considers that the seriousness threshold should match the seriousness threshold contained in the mid-tier of enforcement provisions to be introduced pursuant to proposal 24.1.

Though several international jurisdictions with private rights of action under their domestic privacy laws do not prescribe a particular harm threshold that must be met before an individual can seek redress in the courts,[86] a 'highly offensive to the reasonable person'[87] threshold exists in the United States of America for such breach of privacy claims.

---

[80] *Federal Circuit Court Rules 2001* (Cth) r 45.11; *Fair work: Small claims* (Web page) <https://www.fcfcoa.gov.au/gfl/fairwork-small-claims>.

[81] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Issues Paper No 43, 3 October 2013) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-ip-43/issues-paper-2/a-statutory-cause-of-action-for-serious-invasion-of-privacy/>.

[82] Rachel Callinan. 'Court Delays in NSW: Issues and Developments' (Briefing Paper No 1/02, NSW Parliamentary Library Research Service, January 2022) <https://www.parliament.nsw.gov.au/researchpapers/Documents/court-delays-in-nsw-issues-and-developments/01-02.pdf>.

[83] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Issues Paper No 43, 3 October 2013) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-ip-43/issues-paper-2/a-statutory-cause-of-action-for-serious-invasion-of-privacy/>.

[84] Office of the Australian Information Commissioner, 'Submission to the Attorney-General's Department Paper on the Privacy Act Review Issues Paper' (11 December 2020) <https://www.oaic.gov.au/__data/assets/pdf_file/0018/1773/privacy-act-review-issues-paper-submission.pdf>.

[85] Ibid.

[86] Ibid. See Singapore's Personal Data Protection Act 2012 which provides that any person who suffers loss or damage directly as a result of a contravention of the Act by an organisation shall have a right of action for relief in civil proceedings in a court. See also Article 82 of the GDPR, whereby any person who has suffered material or non-material damage (such as emotional distress) as a result of a violation of the GDPR has the right to compensation.

[87] Restatement (Second) of Torts (1977) (USA), § 652B and § 652D.

In *ABC v Lenah Game Meats*,[88] Gleeson CJ noted that this standard was a 'useful practical test' which involves claimants proving whether the interference is likely to be 'highly offensive' to a reasonable person and is not of legitimate concern to the public.[89] As such, the NSWCCL suggests adopting the US approach to a harm threshold for breaches of privacy under the Privacy Act.

Journalism carve-out

The NSWCCL acknowledges that journalistic acts and practices may clash with this proposed direct right to action. Such a clash is already ameliorated pursuant to s 7B(4) of the Privacy Act, which exempts acts and practices of 'media organisations', subject to certain requirements.

This exemption for journalistic materials or news activities should be retained for the purposes of a direct right to action, which could be achieved subject to a possible defence or exception for 'responsible journalism'. For example, in the US jurisdiction, there is an exception for the tort of invasion of privacy which is whether the information is 'newsworthy'. In other words, if the information or facts in question are a matter of legitimate public concern, then it can be raised as a defence.[90]

26. A STATUTORY TORT OF PRIVACY

Proposal 26.1 (Option 1): ***Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.***

Proposal 26.2 (Option 2): ***Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.***

Proposal 26.3 (Option 3): ***Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.***

Proposal 26.4 (Option 4): ***In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.***

The NSWCCL supports the introduction of a statutory tort for invasion of privacy.

NSWCCL considers that a statutory framework is necessary to ensure that the public's expectation of privacy protection is given form. Currently, the common law has failed to give effect to a tort of privacy invasion, for which there is strong public support.

An extensive and robust statutory tort would address two main mischiefs:

- an intrusion upon seclusion (such as by physically intruding into the plaintiff's private space or by watching, listening to, or recording the plaintiff's private activities or affairs); and

- a misuse of private information (such as by collecting or disclosing private information about the plaintiff).

A fault element of either intention or recklessness should be included in any tort. In addition, a reasonable person in the plaintiff's position must have an expectation of privacy. Crucially, the court would need to be satisfied that the public interest in privacy outweighs any countervailing public interests,[91] which could include freedom of reporting in the media and freedom of political communication and expression.

[88] (2001) 208 CLR 199.

[89] Ibid [42] (Gleeson CJ); Australian Law Reform Commission (n 10).

[90] Samantha Katze, 'Hunting the Hunters: AB 381 and California's Attempt to Restrain the Paparazzi' (2006) 16 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1349.

[91] Recommendation 19, Digital Platforms Report, p493, and Recommendations, ALRC Report

Existing case law has left the door open to the creation of a common law tort of invasion of privacy (*ABC v Lenah Game Meats* 208 CLR 199), yet there has been marked judicial inaction when cases arise in this area (it has been 30 years since the English case of *Kaye v Robertson* [1990] EWCA Civ 21 where the court ruled that privacy had been breached but there was no law under which the breach could be remedied). Such cases include:

- Cases where a misuse of information has led to the court ostensibly appearing to affirm a tort of invasion of privacy. For example, in *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281, the court awarded damages to a victim of sexual assault when her identity was publicly revealed by the ABC. This case was unique because the tort of invasion of privacy ostensibly operated to supplement the privacy act, not as an extension of it.

- Similarly, in Grosse v Purvis (2003) Aust Torts Reports 81-706, a victim of an egregious breach of privacy successfully sued a tortfeasor for damages under a tort of invasion of privacy for conduct that could be described as 'stalking'.

- While the above two cases appear to suggest the existence of such a tort, these decisions have been undermined by cases such as Giller v Procopets [2004] VSC 113, which declined to acknowledge the existence of a tort of invasion of privacy because '*the law has not developed to the point where the law in Australia recognises an action for breach of privacy*'.

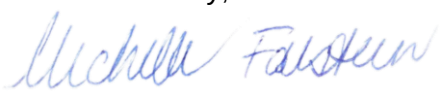
- This refusal of recognition engenders outcomes like those seen Glencore International AG v Commissioner of Taxation [2019] HCA 26, where common-sense expectations of privacy in regards to cybersecurity were only actionable on the basis of a breach of legal professional privilege, as opposed to any kind of invasion of privacy basis.

The history of these cases suggests common law development toward such a tort has been incremental and slow. Introducing a statutory tort would have the effect of declaring the existence of such a tort as well as establishing its boundaries.

The NSWCCL considers such a tort to be necessary to address the ever-growing role of the internet and social media platforms, particularly insofar as they relate to the virtual distribution of invasive material via online platforms. The introduction of a statutory tort will also allow private citizens to better assert their rights even outside of the courthouse (given the existence of firm legal grounds upon which to advance letters of demand).

The NSWCCL also supports the implementation of an offensiveness threshold as it would serve to differentiate similar fact scenarios based on how egregious the conduct (i.e. how far removed the conduct was from general standards of privacy) was. A cultural standard, adopting a principles-based approach to such a threshold would allow for the general principle of right to privacy to be considered, rather than an overarching rules-based or strictly formulaic statute approach which could see innocuous or inadvertent 'invasions' being actionable under such a tort.

Yours sincerely,



Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission- Michelle Falstein
Email: michelle.falstein@nswccl.org.au Mobile: 0412980540