



Australian  
Human Rights  
Commission

# Human Rights in the Digital Age: Additional Material Submitted to the UN Global Digital Compact

Australian Human Rights Commission

Submission to the United Nations' Office of the Secretary-General's  
Envoy on Technology

30 April 2023

ABN 47 996 232 602  
Level 3, 175 Pitt Street, Sydney NSW 2000  
GPO Box 5218, Sydney NSW 2001  
General enquiries 1300 369 711  
Complaints info line 1300 656 419  
TTY 1800 620 241

Australian Human Rights Commission  
[www.humanrights.gov.au](http://www.humanrights.gov.au)



**Contents**

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
<b>2</b>	<b>Consultations .....</b>	<b>4</b>
<b>3</b>	<b>Protection of data.....</b>	<b>5</b>
3.1	<i>Informed consent model.....</i>	<i>5</i>
3.2	<i>Review of existing legislative frameworks .....</i>	<i>7</i>
3.3	<i>Existing work and rights to privacy .....</i>	<i>8</i>
3.4	<i>How new and emerging technologies may risk privacy .....</i>	<i>10</i>
<b>4</b>	<b>Promoting the regulation of artificial intelligence .....</b>	<b>12</b>
4.1	<i>Algorithmic bias.....</i>	<i>12</i>
4.2	<i>AI Safety Commissioner.....</i>	<i>13</i>
4.3	<i>Pessimism towards a timely legislative response.....</i>	<i>15</i>
4.4	<i>Safety by design.....</i>	<i>16</i>
4.5	<i>Impact assessments .....</i>	<i>17</i>
<b>5</b>	<b>Applying human rights online .....</b>	<b>18</b>
5.1	<i>A model for regulation and promotion of human rights.....</i>	<i>19</i>
<b>6</b>	<b>Introducing accountability criteria for discrimination and misleading content .....</b>	<b>20</b>
6.1	<i>Model of regulation .....</i>	<i>20</i>
6.2	<i>Freedom of expression .....</i>	<i>21</i>
<b>7</b>	<b>Recommendations .....</b>	<b>22</b>

# 1 Introduction

1. The Australian Human Rights Commission (Commission) welcomes the opportunity to make this submission to the United Nations Office of the Secretary-General's Envoy on Technology (Envoy) in respect of the Global Digital Compact (Compact).
2. The role of the Commission is to work towards a world in which human rights are respected, protected and promoted. While the Commission has expertise and knowledge in the area of human rights generally, relevant to the Compact, it has also developed specific expertise in respect of the human rights risks posed by digital technologies. Most recently, this can be seen in the Human Rights and Technology Project, which was a three-year, national investigation that culminated with the release of the [Human Rights and Technology Project Final Report in 2021](#) (Final Report).
3. This submission builds on the previous work that the Commission has done to advocate for human rights-centred design and deployment of new and emerging technologies, and demonstrates a commitment to global leadership in respect of human rights in digital spaces.
4. The Commission has continued its work in 2023 on human rights and technology. This submission is in addition to other 2023 submissions to date, including to the:
  - [Select Committee on Foreign Interference through Social Media](#)
  - [Targeted Review of Divisions 270–271 of the Criminal Code Act 1995 \(Cth\)](#) (in respect of technology facilitated crime)
  - [Attorney-General's Department Review Report on the Privacy Act 1988 \(Cth\)](#)
  - [Special Rapporteur on contemporary forms of slavery, including its causes and consequences' Call for input on the use of technology in facilitating and preventing contemporary forms of slavery](#)
  - Australian Competition and Consumer Commission expanding digital platform ecosystem issues paper (pending public release).
5. In this submission the Commission addresses the protection of data, regulation of artificial intelligence, application of human rights online and the introduction of an accountability criteria for discrimination and misleading content. The Commission welcomes further opportunities to provide submissions to the Envoy.

## 2 Consultations

6. Although the views expressed in this submission are those of the Commission, they have been informed by the views and opinions expressed by participants throughout the consultation process.
7. The Commission facilitated two consultations with a range of stakeholders and experts from civil society, business, regulators and government.
8. Participants were provided with a Consultation Note when they were invited to attend the sessions. The Consultation Note set out what the Commission requested stakeholders to bear in mind when engaging in the consultations. It emphasised that participants should consider:
  - input on the core principles that all governments, companies, civil society organizations, and other stakeholders should adhere to in respect of the topic areas.
  - key commitments to bring about these specific principles. These could take the form of what should be done and/or based on what has already been done.
9. The Commission also encouraged invitees to provide written input via email where they were unable to attend the online consultations, or if they wished to further expand upon what was discussed.
10. Each consultation was held via Microsoft Teams and conducted under the 'Chatham House Rule'. Australian Human Rights Commissioner, Lorraine Finlay, provided the introduction to participants while the consultation was facilitated by Human Rights Advisor (Business and Technology), Patrick Hooton.
11. The first consultation was held on Monday, 3 April, and covered the protection of data and the promotion of the regulation of artificial intelligence (AI). The first half of the consultation was dedicated to seeking the views of participants on the protection of data. The second half was utilised to discuss the regulation of AI.
12. The second consultation was held on Thursday, 6 April, and covered applying human rights online and introducing accountability criteria for discrimination and misleading content. The first half of the consultation was dedicated to seeking the views of participants on applying human rights online. The second half discussed the introduction of accountability criteria for discrimination and misleading content.
13. Across the two sessions, 36 participants engaged in the Commission's consultations on the Compact. A further 7 stakeholders provided written submissions.

### 3 Protection of data

14. One of the key issues which must be addressed in protecting data is the consideration of how government and organisations can best protect individual users' data.

#### 3.1 Informed consent model

15. Although there is always a need to improve digital literacy skills to empower people to make informed decisions about how their data is used, this in isolation is insufficient in protecting data. Relying too heavily on digital literacy training places too great an onus on users to protect their data. Models of data protection which seek to place the onus on individuals, and not the organisations that seek to utilise that data, are problematic.

16. Australia has adopted a regulatory model which primarily places the onus on individuals to protect their data. For example, users are often asked to accept the terms and conditions of long and complicated collection notices and privacy policies, in exchange for a product or service.<sup>1</sup> Collection notices are often difficult to understand, making it challenging for users to appreciate what information is being collected and how it may be used. This is supported by the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry – Final Report, which highlighted how lengthy and complex documents were exacerbating issues surrounding transparency.<sup>2</sup>

17. Research has also shown the emergence of 'dark patterns' which confirms that the use of manipulative and deceptive designs can cause significant harm.<sup>3</sup> This can lead to individuals losing control of their data or being manipulated into making choices which are not in their interests.<sup>4</sup>

18. However, even where an individual understands how their data may be used, they are often ill-equipped, in practice, to do anything about it due to the immense power imbalance between 'lonely individuals' and monolithic organisations. There is a very limited ability for individuals to negotiate how their data is used, as such terms are provided on a 'take-it-or-leave-it' basis.

19. This 'take-it-or-leave-it' approach by organisations can lead to excessive data collection inconsistent with the wishes of the individual.<sup>5</sup> It also requires individuals to either accept the terms or not engage with the provided service. In the modern era, where online engagement has become integral to everyday living for many, this is no real 'choice' and doesn't offer meaningful protection of data.<sup>6</sup>

20. Despite being aware, and disapproving, of the risks to privacy, individuals are often unwilling or unable to stop using appliances or services which threaten their privacy.<sup>7</sup> This reluctance or inability to avoid products or services which threaten privacy, may partly be in response to a lack of effective competition or alternative. The ACCC has previously found that a lack of competition and unavailability of reasonable alternatives (which may better protect privacy) can lead users to accept undesirable terms and conditions.<sup>8</sup>
21. Even where an individual understands how their data will be used, this power imbalance remains, as 'one party controls the design of applications and the other must operate within that design'.<sup>9</sup>
22. The Commission would also highlight the impact of the 'privacy paradox': the phenomenon that, despite understanding the privacy risks of a product or service, there is no obvious influence upon an individual's behaviour.<sup>10</sup> Namely, individuals will still engage with privacy-adverse products and services even where they are highly aware of the risks.
23. This does not mean that individuals do not care about their privacy. In fact, data protection is crucial in maintaining trust in digital ecosystems. The Office of the Australian Information Commissioner (OAIC) [Australian Community Attitudes to Privacy Survey 2020](#) report demonstrates that a majority of Australians (around 70%) believe that privacy is a major concern in rapidly evolving digital environments.<sup>11</sup>
24. Moreover, 79% of Australians agree that companies should not be able to sell a users' data under any circumstances. A further 70% are uncomfortable with companies using data to monitor their online behaviours.<sup>12</sup>
25. The above highlights fundamental issues in a model which places the onus on individuals to protect their own data. The Commission is aware of emerging models which move away from such individual-onus-heavy approach.
26. For example, the Consumer Policy Research Centre in its [In whose interest? Why businesses need to keep consumers safe and treat their data with care](#) (Working Paper) put forward two alternative approaches to protecting data in Australia – which may have global application.
27. The Working Paper canvasses the creation of a duty of care or best-interest duty, which would operate similarly to fiduciary duties in the finance sector to hold businesses accountable for how they collect, share and use consumer data.<sup>13</sup>
28. The Working Paper also advocates for a:

Privacy Safety Regime which utilises concepts from product intervention powers and product safety interventions, proposing options that would allow governments and regulators to stop or limit obviously harmful uses of data as well as a process for regulators to proactively restrict and test new harmful practices as they evolve.<sup>14</sup>

29. While the Working Paper is specific to Australia, the Commission would call upon the Envoy to consider how similar models may be applicable, or could be adapted, to inform the better protection of data globally.

**Recommendation 1: Countries must consider models for protecting data and personal information online which do not place the primary onus on individuals to actively protect their personal information.**

### **3.2 Review of existing legislative frameworks**

30. In 2023, the Australian Government Attorney-General's Department released the [final report of its review of the Privacy Act 1988 \(Cth\)](#) which considered whether Australia's privacy legislation was fit for purpose. This review recognised that Australians now live much of their lives online, where their information is collected and used for a myriad of purposes in the digital economy.

31. The *Privacy Act 1988 (Cth)* (Privacy Act) is a key legislative protection of individuals' personal information in Australia. The 13 Australian Privacy Principles (APPs) are structured to reflect privacy obligations across the information lifecycle, as entities collect, hold, use, disclose, and destroy or de-identify personal information. The APPs are legally binding principles, which provide entities with the flexibility to take a risk-based approach to compliance based on their particular circumstances, including size, resources and business model, while ensuring the protection of individuals' privacy.

32. In considering how best to protect data, proactive reviews of key privacy legislation is essential. Countries must regularly review their key pieces of privacy legislation to ensure it is modern, fit for purpose and drafted in a technology neutral manner.

**Recommendation 2: Countries should regularly engage in consultative reviews of the legislation which regulates privacy and data. Such**



**reviews should specifically consider if the relevant legislation is technology neutral.**

### **3.3 Existing work and rights to privacy**

33. In a written submission, one stakeholder highlighted existing work that should inform the development of the Compact:

As the United Nations considers the core principles that governments, companies, civil society organisations and other stakeholders should adhere to in relation to data protection, it may find it helpful to consider the work of Data Protection Authorities in this space. In 2009 the International Conference of Data Protection and Privacy Commissioners (now called the Global Privacy Assembly, or GPA) passed a [resolution](#) recognising the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data as a set of principles, rights, obligations and procedures that any legal system of data protection and privacy should strive to meet (the Madrid Resolution).

The purpose of the Madrid Resolution was to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data and to facilitate the international flows of personal data needed in a globalized world. The GPA's Global Frameworks and Standards Working Group is undertaking work towards a resolution or policy statement to articulate the GPA's view of high data protection and privacy standards, including through reviewing the Madrid Resolution. While its work is in its initial stages, the Madrid Resolution's content is quite comprehensive and forward-thinking. It may therefore be useful for the UN to consider the Madrid Resolution, as well as the ongoing work of the GPA.

**Recommendation 3: The Envoy should apply the Madrid Resolution and the ongoing work of the GPA in developing the Compact.**

34. The right to privacy is a human right under article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), as well as being enshrined in a number of other applicable international human rights instruments.<sup>15</sup> The human right to privacy must be central to any discussion of how to best protect data.

**Recommendation 4: The Envoy should have regard to article 17 of the ICCPR in developing the Compact.**

35. The importance of accessibility of technology for vulnerable people and ensuring that people with disability can also engage in modern living without their privacy being placed at risk, was raised during the consultations. Article 22 of the *Convention on the Rights of Persons with Disabilities* was raised to highlight the importance of the respect for privacy for people with disability. Equally, article 16 of the *Convention on the Rights of the Child* is of significance in protecting children and young people's privacy. This will be especially important when developing the Compact.

**Recommendation 5: The Envoy should have regard to article 22 of the *Convention on the Rights of Persons with Disabilities* and article 16 of the *Convention on the Rights of the Child* in developing the Compact.**

36. The Commission launched a [Position Paper: A Human Rights Act for Australia](#) (Position Paper) on 9 March 2023. In the Position Paper the Commission recommends the inclusion of a 'right to privacy and reputation' in its proposed Australian Human Rights Act.<sup>16</sup> Australia does not currently have a federal human rights act.

37. The proposed right to privacy and reputation outlined in the proposed model for a Human Rights Act states:

*A person has the right-*

*(a) not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and*

*(b) not to have the person's reputation unlawfully attacked.*

*Note: The right to privacy applies to the collection, processing or retention of personal data through all forms of technology, and includes state surveillance measures.<sup>17</sup>*

38. This proposed right to privacy and reputation implements article 17 of the ICCPR (to which Australia has signed and ratified).<sup>18</sup>

39. Pertinently, the note clarifies that privacy rights extend to technological surveillance measures, noting the increased capacity of the state collect personal data and make decisions based on that data through AI.<sup>19</sup>

40. In protecting data, the protection of the human right to privacy should be enshrined in domestic legislation, in addition to existing international obligations, to best protect user data.

**Recommendation 6: Countries should ensure that their domestic legal framework includes protection for the right to privacy, with specific regard for the collection and use of data.**

### 3.4 How new and emerging technologies may risk privacy

41. There is a serious need to consider the protection of data in respect of new and emerging technologies. The Metaverse is one prominent example of a new technology which threatens privacy. The Metaverse utilises virtual reality (VR) goggles and other technologies that are able to collect an unprecedented level of personal information.

42. While the Commission has raised previous concerns about the erosion of privacy in digital spaces,<sup>20</sup> the Metaverse creates an unprecedented risk to privacy and data. The risk of privacy and security invasions in the Metaverse (inherited from underlying technologies or emerging from the new digital ecology) may be prolific.<sup>21</sup>

43. The Metaverse is a nebulous digital construct which is constantly evolving – but broadly speaking it can be considered as the next generation of the internet with the aim to be a fully immersive, hyper-spatiotemporal, and self-sustaining virtual shared space for humans to play, work, and socialize.<sup>22</sup> This allows individual users to live as ‘digital natives’ and experience an alternative virtual life,<sup>23</sup> while at the same time having the ability to facilitate transactions and activities that also have a presence in the physical world.

44. The personal data involved in the Metaverse will likely be ‘more granular and unprecedentedly ubiquitous to build a digital copy of the real world’.<sup>24</sup> The fusion of this granular data collected by Metaverse technologies and more traditional data collected by social networking platforms may compromise privacy at heightened levels. Such a fusion, or interoperability of data, may create unpredictably deeper data profiles about individuals.<sup>25</sup>

45. The Metaverse collects and processes vast amounts of data such as:

- biometrics
- facial expressions
- eye movements

- iris movements
- hand movements
- speech
- brain wave patterns
- habits
- choices
- activities of users
- behaviours
- feelings
- expressions
- user conversations
- internet history
- body movements
- cultural data
- financial data
- communications
- location
- age
- shopping preferences
- favourite movies
- identities
- medical data
- digital assets
- the identity of virtual items
- cryptocurrency spending records
- physiological data
- physical data.<sup>26</sup>

46. Even the motion sensors and cameras usually built into VR helmets, which help track head direction and movement, will draw an individual's room and monitor that space while being used.<sup>27</sup>

47. The collection of such vast and intrusive information will undoubtedly bring into question the protection of personal data in the Metaverse.<sup>28</sup> However,

the Metaverse is only one example of a new and emerging technology which may pose an increased risk to privacy and data online.

48. This highlights the need for technology neutral legislation to adapt to new and emerging technologies.

**Recommendation 7: Privacy legislation must be drafted in technology-neutral terms.**

## 4 Promoting the regulation of artificial intelligence

49. There are numerous human rights risks associated with the unregulated use of AI. The following risks of AI are especially relevant:

- malicious use of an AI tool to commit crime or cause harm
- enhanced surveillance that poses risks to privacy and human dignity
- safety risks and damage from negligence
- harm to consumers
- concerns about automation of decision-making, including bias and reduced accountability
- potential threats to democracy
- reduced employment for humans
- potential threats from artificial general intelligence.<sup>29</sup>

50. These are just some of the risks which in-part justify the need for regulation of AI. The Commission is especially concerned about the role that algorithmic bias plays in entrenching discrimination.

### 4.1 Algorithmic bias

51. While AI allows large amounts of relevant information to be considered in decision-making processes and may encourage efficient, data-driven decision making, its regulation is becoming increasingly important, due to its potential to produce 'algorithmic bias'. Algorithmic bias arises where an AI tool produces outputs that result in unfairness.<sup>30</sup> Algorithmic bias can entrench unfairness, or even result in unlawful discrimination.<sup>31</sup>

52. AI systems may unintentionally produce discrimination in the employee vetting process. For instance, Amazon used an AI software that was designed to review resumes and determine which applicants Amazon should hire.<sup>32</sup> The algorithm systemically discriminated against women applying for technical jobs, such as software engineer positions. This is because the existing pool of Amazon software engineers were by majority male, and as such, the new software was fed data about those engineers' resumes.<sup>33</sup> The practice of directing software to discover resumes that harbor similarities to resumes in a training data set will inevitably reproduce the demographics of the existing workforce.<sup>34</sup>
53. Another example of algorithmic bias was when, in 2019, a study discovered that a clinical algorithm used by many hospitals in the US to determine which patients required extra medical care produced racial bias.<sup>35</sup> The algorithm was trained on past data on healthcare spending, which reflects a trend whereby black patients have less income to spend on their healthcare as compared with white patients - a result of systemic wealth and income disparities.<sup>36</sup> As such, the algorithm's outputs reflected a discriminatory result whereby white patients required more medical care than black patients.<sup>37</sup>
54. Such examples highlight why AI requires greater regulation, in the interests of increasing transparency and preventing unfairness and unlawful discrimination in algorithmic decision-making. This is especially the case given the difficulty of applying anti-discrimination laws to complex AI systems.<sup>38</sup> The Commission emphasises its 2020 technical paper [Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias](#) which considers algorithmic bias in greater detail.

## 4.2 AI Safety Commissioner

55. In responding to how AI can be regulated countries should, at first instance, modify their existing laws, regulations and regulatory bodies in a manner which better allows them to respond to the risks posed by AI. However, this is a short-term response, and there will ultimately need to be an AI-specific statutory body to respond to new and emerging risks in this area.
56. The Commission notes recommendations 22 and 23 of its [Final Report](#).<sup>39</sup> Recommendation 22 stated:
- The Australian Government should establish 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. The AI Safety Commissioner should:

- (a) work with regulators to build their technical capacity regarding the development and use of AI in areas for which those regulators have responsibility
- (b) monitor and investigate developments and trends in the use of AI, especially in areas of particular human rights risk
- (c) provide independent expertise relating to AI and human rights for Australian policy makers
- (d) issue guidance to government and the private sector on how to comply with laws and ethical requirements in the use of AI.<sup>40</sup>

57. Moreover recommendation 23 continued that:

The AI Safety Commissioner should:

- (a) be independent from government in its structure, operations and legislative mandate, but may be incorporated into an existing body or be formed as a new, separate body
- (b) be adequately resourced, wholly or primarily by the Australian Government
- (c) be required to have regard to the impact of the development and use of AI on vulnerable and marginalised people in Australia
- (d) draw on diverse expertise and perspectives including by convening an AI advisory council.<sup>41</sup>

58. The Commission considers that an AI Safety Commissioner could address three major needs:

First, government agencies and the private sector are often unclear on how to develop and use AI lawfully, ethically and in conformity with human rights. An AI Safety Commissioner could provide expert guidance on how to comply with laws and ethical standards that apply to the development and use of AI.

Secondly, regulators face the challenge of fulfilling their functions even as the bodies they regulate make important changes to how they operate. An AI Safety Commissioner could play a key role in building the capacity of existing regulators and, through them, of the broader 'regulatory ecosystem' to adapt and respond to the rise of AI.

Thirdly, legislators and policy makers are under unprecedented pressure to ensure Australia has the right law and policy settings to address risks and take opportunities connected to the rise of AI. An AI Safety Commissioner could monitor trends in the use of AI here and overseas. This would help it to be a source of robust, independent expertise.

As an independent statutory office that champions the public interest, including human rights, an AI Safety Commissioner could help build public trust in the safe use of AI.<sup>42</sup>

59. A more detailed explanation of the role of an AI Safety Commissioner can be found at pages 125–135 of the Final Report.

60. Although the above is specific to Australia, the notion is applicable more broadly. All countries would benefit from the creation of such an independent statutory body to better promote the regulation of AI within their countries.

**Recommendation 8: Countries should establish statutory bodies specifically focused on promoting and protecting human rights in respect of AI. These statutory bodies should also work towards advancing AI regulation. Such bodies must be independent and appropriately funded.**

61. However, the creation of such a body will take time. In the meantime, countries must build upon the capacity of existing regulators.

**Recommendation 9: Until an independent statutory body, as described in Recommendation 8 is implemented, countries must build the capacity of existing regulators, including by increasing funding, to better respond to the human rights risks of AI.**

### 4.3 Pessimism towards a timely legislative response

62. The Commission is alarmed by the rise of generative AI, and stresses that this necessitates an effective and fast response to its regulation. This is supported by the Future of Life's [Pause Giant AI Experiments: An Open Letter](#) which calls on:

all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4. This pause should be public and verifiable, and include all key actors. If such a pause cannot be enacted quickly, governments should step in and institute a moratorium.<sup>43</sup>

63. Unfortunately the open letter is unlikely to have any real effect in regulating AI, or addressing potential risks of AI, due to its non-binding nature. It is also questionable if any governments are even capable of



enforcing a moratorium at such short notice. The inability of legislation and regulation to respond in a timely manner to new and emerging technologies is disappointing. However, countries should still pursue legislative responses aimed at regulating AI.

64. It is important to note that some have indicated that regulation may stymie innovation in the AI space. However, the Commission would emphasise that not all regulation is anti-innovation. In fact, it is often the case that regulation may stimulate innovation and promote, rather than restrict, new activity.<sup>44</sup>

#### 4.4 Safety by design

65. The Compact should consider upstream solutions to the risks of AI in the design and development phases of AI products. This mitigates the risk of harms occurring at later stages when AI products are deployed.

66. The Commission would point to the eSafety Commissioner's work in ensuring that technology companies apply [Safety by Design](#). This initiative positions individual user safety and rights as a central component in the design and deployment of digital products and services.<sup>45</sup> It seeks to alter the technology industry's 'move fast and break things' ethos.<sup>46</sup>

67. Safety by Design includes a set of three fundamental Safety by Design principles:

- **Service provider responsibilities:** The burden of safety should never fall solely upon the user. Online service providers must take reasonable steps to ensure a safe digital environment for users, in addition to having clear ways for individuals to lodge complaints.
- **User empowerment and autonomy:** The dignity of users is of central importance. Products and services should align with the best interests of all users online.
- **Transparency and accountability:** Transparency and accountability are hallmarks of a robust approach to safety. This ensures product and service providers operate in accordance with their published safety objectives, and assists in educating and empowering users about how they can address safety concerns.<sup>47</sup>

68. This initiative is heavily influenced by human rights, digital ethics and the need to design online environments which are human-centric.<sup>48</sup> As all countries grapple with the risks posed by the meteoric rise of technological advancements, Safety by Design should be proactively considered during the design and development of products and services.

69. Such principles demonstrate the importance of proactive and human rights-centred design and deployment of technology. Recognition and commitment to such principles within the Compact would go far in mitigating the harms of AI.

**Recommendation 10: The Compact recognise and include the eSafety Commissioner’s Safety by Design Principles.**

## 4.5 Impact assessments

70. In the Commission’s Final Report, it was recommended that the AI Safety Commissioner should develop a tool to assist private sector bodies undertake human rights impact assessments (HRIAs) in developing AI informed decision-making systems. This included recommending that the Australian Government should maintain a public register of completed HRIAs.<sup>49</sup>

71. HRIA tools assess how a new product, service, law or policy will engage human rights. They also provide a framework for ensuring adequate rights protections.

72. As noted in the Final Report:

HRIAs are increasingly being used by government, the private sector and civil society organisations to measure the risk to human rights posed by their activities, ensure that measures are put in place to address human rights risks, and support the availability of remedies for any human rights infringements.<sup>50</sup>

73. The Commission’s previous work has found strong support from the public and private sectors, for the Australian Government to develop an HRIA tool and associated guidance for AI-informed decision making.<sup>51</sup>

74. Although the Commission’s work in advancing HRIAs in respect of AI has been specific to the Australian jurisdiction, the use of HRIAs globally would help to identify and address human rights issues at the earliest stage of the design in AI-informed decision-making systems.

**Recommendation 11: HRIAs should be conducted when developing all AI products.**

## 5 Applying human rights online

75. A common theme that emerged in the consultations was the diversity of human rights that were relevant online. Specific rights that were discussed as being particularly significant in the online context included:

- freedom of expression
- cyberbullying
- internet freedom
- access to digital infrastructure
- privacy online
- digital exclusion
- freedom of assembly
- freedom of association.

76. It is important to note that the broader discussion of human rights online can often become limited to a narrow understanding of freedom of expression and the right to privacy. When examining this discourse, it is crucial to carefully consider how the rights to privacy and free expression may manifest differently for different individuals and groups.

77. Moreover, legal frameworks which protect human rights (such as privacy and safety laws) are not mutually exclusive, as tensions may exist as between these frameworks. Where tensions do exist across frameworks, they should be examined and addressed in a way that is proportionate and gives effect to the objectives of protecting and promoting human rights.

78. In promoting human rights online, countries need to apply existing rights to these online spaces, in lieu of developing new human rights which were modified for new and emerging technologies. Specific regard should also be held for how tensions between rights and frameworks are considered.

**Recommendation 12: To promote human rights in digital ecosystems, the Compact should apply pre-existing human rights – as opposed to creating novel rights only applicable to online environments.**

79. Existing human rights already apply offline, however they must also apply in the whole digital ecosystem – and not just on the internet or in relation to specific online spaces or products.

**Recommendation 13: Human rights must apply to the whole digital ecosystem.**

**5.1 A model for regulation and promotion of human rights**

80. Unlike in non-digital environments, no individual government bears primary responsibility or accountability for the maintenance of human rights online. These digital spaces are primarily run by private businesses who do not bear the same responsibility as governments. This complicates how human rights can be protected online.
81. One method to best protect human rights online is to ensure that all stakeholders engage in human rights-centred design and deployment of new and emerging technologies.

**Recommendation 14: Stakeholders must commit to human rights-centred design and deployment of new and emerging technologies.**

82. Co-regulation is sometimes referred to as enforced self-regulation, that is enforced, or threatened to be enforced, by a regulator or government.<sup>52</sup> Co-regulation utilises the know-how of those within industry, but ensures an external oversight mechanism to encourage compliance.<sup>53</sup> Self-regulation without the threat of enforcement by a regulator has led to a formidable history of industry abuse of the self-regulation privilege.<sup>54</sup>
83. To best ensure that human rights can be applied, and protected, an online model which focuses on co-regulation is preferred over self-regulation. It will also be important to ensure that relevant stakeholders are consulted with when drafting or applying any model of promoting human rights online.

**Recommendation 15: Any model for regulation which seeks to protect human rights online must adopt a co-regulatory model. Such a model should be developed in collaboration with relevant stakeholders.**

84. When discussing these rights, regard must be had for vulnerable people and people with disability who are often unable to fully enjoy the benefits of new and emerging technologies. Regard must also be had for the

maintenance and protection of human rights for all people including children, young people, elderly people, indigenous people, people with disability and people without access to technology or internet.

**Recommendation 16: The Compact must ensure that all people can reap the benefits of new technologies – while also having their human rights promoted and protected.**

## 6 Introducing accountability criteria for discrimination and misleading content

85. The Commission questions how discriminatory and misleading content can be effectively countered online. Combatting such content implicitly requires a right of reply – which does not automatically exist on digital platforms given their private ownership. The time it takes to disprove misleading content is also too long when compared to how quickly, and efficiently, such misleading content can be created and circulated.

### 6.1 Model of regulation

86. The Human Rights Law Centre's recent [submission to the inquiry into the influence of international digital platforms](#) notes the role that social media platforms play in driving the spread of disinformation and hate speech.

87. Although Australia has been a world leader in establishing the e-Safety Commissioner (which is Australia's independent regulator for online safety and is the world's first government agency dedicated to keeping people safer online),<sup>55</sup> Australia and other countries lag in regulating discrimination, hate speech and misleading content on digital platforms.

88. One of the recommendations of the Human Rights Law Centre's [submission to the inquiry into the influence of international digital platforms](#) was a move away from self-regulatory and co-regulatory models for digital platforms, by replacing existing co-regulatory codes and ensuring new regulations are written by legislators or regulators.

89. The submission further noted that:

In the EU, the introduction of the Digital Services Act was driven by growing recognition that self- and co-regulatory models are inadequate and ineffective. ... Regulator-drafted industry standards should be the norm. ... It is essential that the regulation of digital

platforms in Australia evolve toward an enforceable legal framework drafted by regulators and lawmakers and overseen by an appropriately resourced and empowered regulator.<sup>56</sup>

90. This view differs from the co-regulatory model proposed in respect of human rights more broadly. However, the move away from a co-regulatory model in respect of countering discriminatory and misleading content is needed due to the profound harm it causes and difficulty in policing it. The Compact must recognise the need for countries to introduce domestic legislation which provides an enforceable legal framework to counter discriminatory and misleading content.

**Recommendation 17: Countries should introduce enforceable domestic legislation which requires social media platforms to better counter discriminatory and misleading content.**

91. Again, a large part of combatting discriminatory and misleading content online is by developing and deploying technologies which are not discriminatory or misleading in the first place – or that are at least capable of combatting such content upon deployment.

## **6.2 Freedom of expression**

92. Social media platforms, which function as a digital ‘town square’ for free speech and self-expression, are increasingly affected by censorship. The right to freedom of expression is often challenged in digital commons as users seek to express their views on a wide range of topics.

93. However, there is often a competing tension on where to draw the line between freedom of expression and content moderation. This is a line where reasonable minds may differ – however moderation should not unduly impact free speech, nor should hateful content be allowed to prosper under the guise of freedom of expression.

94. Transparency is the key to ensuring that any regulation which censors content does not unduly restrict the exercise of free speech. Where top-down regulation is utilised to counter discriminatory and misleading content, such regulation must maintain transparency in how they determine what content is to be moderated or censored to avoid producing a chilling effect on freedom of expression and democratic engagement online.

**Recommendation 18: Domestic legislation aimed at countering discriminatory and misleading content online must transparently set out how content is moderated and censored to avoid a chilling effect on free speech and democratic discourse.**

## 7 Recommendations

95. The Commission makes the following recommendations.

### **Recommendation 1**

Countries must consider models for protecting data and personal information online which do not place the primary onus on individuals to actively protect their personal information.

### **Recommendation 2**

Countries should regularly engage in consultative reviews of the legislation which regulates privacy and data. Such reviews should specifically consider if the relevant legislation is technology neutral.

### **Recommendation 3**

The Envoy should apply the Madrid Resolution and the ongoing work of the GPA in developing the Compact.

### **Recommendation 4**

The Envoy should have regard to article 17 of the ICCPR in developing the Compact.

### **Recommendation 5**

The Envoy should have regard for article 22 of the *Convention on the Rights of Persons with Disabilities* and article 16 of the *Convention on the Rights of the Child* in developing the Compact.

### **Recommendation 6**

Countries should ensure that their domestic legal framework includes protection for the right to privacy, with specific regard for the collection and use of data.

### **Recommendation 7**

Privacy legislation must be drafted in technology neutral terms.

### **Recommendation 8**

Countries should establish statutory bodies specifically focused on promoting and protecting human rights in respect of AI. These statutory bodies should

also work towards advancing AI regulation. Such bodies must be independent and appropriately funded.

**Recommendation 9**

Until an independent statutory body, as described in Recommendation 8 is implemented, countries must build the capacity of existing regulators, including by increasing funding, to better respond to the human rights risks of AI.

**Recommendation 10**

The Compact recognise and include the eSafety Commissioner’s Safety by Design Principles.

**Recommendation 11**

HRIAs should be conducted when developing all AI products.

**Recommendation 12**

To promote human rights in digital ecosystems, the Compact should apply pre-existing human rights – as opposed to creating novel rights only applicable to online environments.

**Recommendation 13**

Human rights must apply to the whole digital ecosystem.

**Recommendation 14**

Stakeholders must commit to human rights-centre design and deployment of new and emerging technologies.

**Recommendation 15**

Any model for regulation which seeks to protect human rights online must adopt a co-regulatory model. Such a model should be developed in collaboration with relevant stakeholders...

**Recommendation 16**

The Compact must ensure that all people can reap the benefits of new technologies – while also having their human rights promoted and protected.

**Recommendation 17**

Countries should introduce enforceable domestic legislation which requires social media platforms to better counter discriminatory and misleading content.

**Recommendation 18**



Domestic legislation aimed at countering discriminatory and misleading content online must transparently set out how content is moderated and censored to avoid a chilling effect on free speech and democratic discourse.

## Human Rights in the Digital Age: Additional Material Submitted to the UN Global Digital Compact, 30 April 2023

### Endnotes

---

- <sup>1</sup> Consumer Policy Research Centre, 'Not a Fair Trade: Consumer views on how Businesses use their Data' (Working Paper, March 2023) 4.
- <sup>2</sup> Australian Competition and Consumer Commission ('ACCC'), 'Digital Platforms Inquiry – Final Report' (Commonwealth of Australia, Final Report, July 2019) 401–428.
- <sup>3</sup> Consumer Policy Research Centre, 'Duped by Design – Manipulative online design: Dark patterns in Australia' (Paper, June 2022) 6.
- <sup>4</sup> Consumer Policy Research Centre, 'In whose interest? Why businesses need to keep consumers safe and treat their data with care' (Working Paper, March 2023) 4.
- <sup>5</sup> ACCC, 'Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers' (Commonwealth of Australia, Issues Paper, March 2023) 7-8.
- <sup>6</sup> Consumer Policy Research Centre, 'Not a Fair Trade: Consumer views on how Businesses use their Data' (Working Paper, March 2023) 4.
- <sup>7</sup> Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' 128 *Computers & Security* (2023) 1.
- <sup>8</sup> ACCC, 'Digital Platform Services Inquiry – September 2023 Report on the expanding ecosystems of digital platform service providers' (Commonwealth of Australia, Issues Paper, March 2023) 7 citing ACCC, *Digital Platform Services Inquiry Fifth Interim Report* (Commonwealth of Australia, Fifth Interim Report, 11 November 2022) 44.
- <sup>9</sup> Consumer Policy Research Centre, 'In whose interest? Why businesses need to keep consumers safe and treat their data with care' (Working Paper, March 2023) 10 citing Jack Balkin, 'The fiduciary model of privacy' 134(11) *Harvard Law Review Forum* (2020) 12.
- <sup>10</sup> Li Li, et al., 'I will only know after using it: The repeat purchasers of smart home appliances and the privacy paradox problem' 128 *Computers & Security* (2023) 1.
- <sup>11</sup> Office of the Australian Information Commissioner ('OAIC'), 'Australian Community Attitudes to Privacy Survey 2020' (Commonwealth Government of Australia, Report September 2020) 4.
- <sup>12</sup> Consumer Policy Research Centre, 'Not a Fair Trade: Consumer views on how Businesses use their Data' (Working Paper, March 2023) 4.
- <sup>13</sup> Consumer Policy Research Centre, 'In whose interest? Why businesses need to keep consumers safe and treat their data with care' (Working Paper, March 2023) 4.
- <sup>14</sup> Consumer Policy Research Centre, 'In whose interest? Why businesses need to keep consumers safe and treat their data with care' (Working Paper, March 2023) 4.
- <sup>15</sup> See e.g. *Universal Declaration of Human Rights*, article 12.
- <sup>16</sup> Australian Human Rights Commission ('AHRC'), 'Free & Equal Position Paper: A Human Rights Act for Australia' ('Position Paper') (Position Paper, March 2023) 111 & 347.
- <sup>17</sup> AHRC, Position Paper (Position Paper, March 2023) 111 & 347.
- <sup>18</sup> AHRC, Position Paper (Position Paper, March 2023) 347.
- <sup>19</sup> AHRC, Position Paper (Position Paper, March 2023).
- <sup>20</sup> See generally AHRC, 'Safeguarding the right to privacy in Australia' Submission to Attorney-General's Department Privacy Act Review Report <<https://humanrights.gov.au/our-work/legal/submission/safeguarding-right-privacy-australia>>.
- <sup>21</sup> Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.
- <sup>22</sup> Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.
- <sup>23</sup> Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 319.

- <sup>24</sup> Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 320; see also Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 82.
- <sup>25</sup> Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
- <sup>26</sup> Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
- <sup>27</sup> Yuntao Wang, et al., 'A Survey on Metaverse: Fundamentals, Security, and Privacy' (2023) 25(1) *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials* 334.
- <sup>28</sup> Yavuz Canbay, Anil Utku & Pelin Canbay, 'Privacy Concerns and Measures in Metaverse: A Review' *15th International Conference on Information Security and Cryptography* (Conference Paper, 2022) 84.
- <sup>29</sup> Michael Guihot & Lyria Bennett Moses, 'Artificial Intelligence, Robots and the Law' 2020 *LexisNexis Australia* 319.
- <sup>30</sup> AHRC, 'Human Rights and Technology Final Report 2021' ('Final Report') (Final Report, 2021) 13.
- <sup>31</sup> AHRC, Final Report (Final Report, 2021) 13.
- <sup>32</sup> Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) <https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against>.
- <sup>33</sup> Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) <https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against>.
- <sup>34</sup> Rachel Goodman, 'Why Amazon's Automated Hiring Tool Discriminated Against Women', *American Civil Liberties Union* (online, 12 October 2018) <https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against>.
- <sup>35</sup> Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) <https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism>.
- <sup>36</sup> Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) <https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism>.
- <sup>37</sup> Crystal Grant, 'Algorithms are Making Decisions About Health Care, Which May Only Worsen Medical Racism' *American Civil Liberties Union* (online, 3 October 2022) <https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism>.
- <sup>38</sup> AHRC, Final Report (Final Report, 2021) 108.
- <sup>39</sup> See generally AHRC, Final Report (Final Report, 2021) 125-135.
- <sup>40</sup> AHRC, Final Report (Final Report, 2021) 128.
- <sup>41</sup> AHRC, Final Report (Final Report, 2021) 129.
- <sup>42</sup> AHRC, Final Report (Final Report, 2021) 125.
- <sup>43</sup> Future of Life Institute, 'Pause Giant AI Experiments: An Open Letter' (Open Letter, 22 March 2023).

- <sup>44</sup> Michael Guihot & Lyria Bennett Moses, 'Artificial Intelligence, Robots and the Law' 2020 *LexisNexis Australia* 322.
- <sup>45</sup> OAIC, 'Safety by Design' (Webpage) <<https://www.esafety.gov.au/industry/safety-by-design>>.
- <sup>46</sup> OAIC, 'Safety by Design' (Webpage) <<https://www.esafety.gov.au/industry/safety-by-design>>.
- <sup>47</sup> OAIC, 'Principles and Background' (Webpage) <<https://www.esafety.gov.au/industry/safety-by-design/principles-and-background>>.
- <sup>48</sup> OAIC, 'Principles and Background' (Webpage) <<https://www.esafety.gov.au/industry/safety-by-design/principles-and-background>>.
- <sup>49</sup> AHRC, Final Report (Final Report, 2021) 98.
- <sup>50</sup> AHRC, Final Report (Final Report, 2021) 98.
- <sup>51</sup> See generally AHRC, Final Report (Final Report, 2021).
- <sup>52</sup> Michael Guihot & Lyria Bennett Moses, 'Artificial Intelligence, Robots and the Law' 2020 *LexisNexis Australia* 327.
- <sup>53</sup> Michael Guihot & Lyria Bennett Moses, 'Artificial Intelligence, Robots and the Law' 2020 *LexisNexis Australia* 327 citing Fiona Haines, 'Regulation and Risk' in Peter Drahos, 'Regulatory Theory: Foundations and Applications' *ANU Press*.
- <sup>54</sup> Michael Guihot & Lyria Bennett Moses, 'Artificial Intelligence, Robots and the Law' 2020 *LexisNexis Australia* 327 quoting John Braithwaite, 'Types of Responsiveness' in Peter Drahos, 'Regulatory Theory: Foundations and Applications' *ANU Press* 117, 124.
- <sup>55</sup> E-Safety Commissioner, 'Who are we' (Web Page) <<https://www.esafety.gov.au/about-us/who-we-are>>.
- <sup>56</sup> Human Rights Law Centre, Submission No 50 to the *Senate Economics Reference Committee* (2023) 9.