Naciones Unidas A/HRC/58/58/Add.2

Asamblea General

Distr. general
2 de abril de 2025
Español
Original: inglés

Consejo de Derechos Humanos
58º período de sesiones
24 de febrero a 4 de abril de 2025
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Visita a Australia

Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères* **

Resumen

La Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères, visitó Australia del 8 al 19 de agosto de 2024. A pesar de que la labor realizada por Australia para poner al día su marco de privacidad en materia de datos personales ha sido un proceso largo, si se priorizan y aplican las principales recomendaciones surgidas del proceso de examen de la Ley de Privacidad, la ley federal en este ámbito se verá reforzada con miras a armonizar el derecho a la privacidad en el plano nacional con el sólido marco de principios de privacidad que existe en el plano internacional. Además, si el Gobierno puede desplegar la voluntad política y los recursos necesarios, también podría ocuparse de la armonización jurisdiccional entre los planos federal y estatal/territorial de la ley de privacidad, y convertirse en un ejemplo para otros Estados federalistas. La Relatora Especial insta a Australia a que introduzca una ley federal de derechos humanos que estreche el vínculo con el marco jurídico internacional con objeto de crear mayor conciencia, reforzar las medidas de protección y posibilitar que la ciudadanía pueda impugnar las presuntas vulneraciones, también del derecho a la privacidad, recurriendo a la Comisión de Derechos Humanos de Australia y, en caso necesario, a los tribunales, para obtener reparación. En el presente informe, la Relatora Especial hace hincapié en que es necesario comprender la interseccionalidad existente entre la dignidad personal y el género, el origen étnico, la edad y la discapacidad, ya que los grupos vulnerables corren un mayor riesgo de ver vulnerada su privacidad, tanto en línea como fuera de ella, lo cual puede evidenciar unas tendencias alarmantes en lo que se refiere a la discriminación, la violencia, la explotación sexual, el ciberacoso y la manipulación financiera. En el informe figuran recomendaciones que abarcan los ámbitos siguientes: los datos personales (incluidos los datos relativos a la salud); el impacto de las tecnologías emergentes en la privacidad; la ciberseguridad y la vigilancia; y el género, los niños y los grupos vulnerables.

* El resumen del presente informe se distribuye en todos los idiomas oficiales. El informe propiamente dicho, que figura en el anexo, se distribuye únicamente en el idioma en que se presentó.

** La oficina pertinente presentó este informe a los servicios de conferencias fuera de plazo por motivos técnicos ajenos a su voluntad.

Anexo

Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères, acerca de su visita a Australia

I. Introduction

1. The Special Rapporteur on the right to privacy, Ana Brian Nougrères, conducted an official country visit to Australia from 8 to 19 August 2024. In the present report, the Special Rapporteur builds on the preliminary observations contained in her press statement issued on 23 August 2024[1] and reflects updated information gathered from engagement with all stakeholders.

2. The Special Rapporteur thanks the Government of Australia for its support, in particular the Attorney-General's Department, the key interlocutor, as the discussions with the authorities were held in a constructive manner. She also thanks all stakeholders who presented her with detailed information and additional documentation in follow-up to her visit. The Special Rapporteur welcomed the opportunity to examine, in detail, the extensive review process in relation to the Privacy Act 1988 with the objective of identifying lessons learned and good practices.

3. The Special Rapporteur had meetings with the Department of the Prime Minister and Cabinet, the Department of Foreign Affairs and Trade, the Attorney-General's Department, the Department of Treasury, the Department of Home Affairs, the National Office of Cyber Security, the Australian Federal Police, the Australian Criminal Intelligence Commission, the Inspector-General of Intelligence and Security, the Department of Finance, the Department of Social Services, the Department of Industry, Science and Resources, the Digital Transformation Agency, the Department of Education, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, the eSafety Commissioner, the National Indigenous Australians Agency, state and territory representatives, the Australian Law Reform Commission, the Federal Court of Australia, the Australian Human Rights Commission, the Office of the Australian Information Commissioner, including the Privacy Commissioner, state and territory privacy commissioners, the National Identity and Cyber Support Service of Australia and New Zealand, the University of Sydney Law School, the University of New South Wales Public Interest Law and Tech Initiative, the Office of the Victorian Information Commissioner, the Victorian Equal Opportunity and Human Rights Commission, the United Nations Association of Australia and numerous academics and civil society organizations.

II. International, regional and national law regarding privacy

A. International and regional law

4. The right to privacy is enshrined in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, which state that no one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon their honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks. In 1980, Australia ratified the International Covenant on Civil and Political Rights, but has not introduced it into domestic law. In 1990, Australia ratified the Convention on the Rights of the Child, which enshrines the right to privacy in article 16 thereof.

[1] See https://www.ohchr.org/en/press-releases/2024/08/australia-must-catch-un-expert-urges-implementation-long-overdue-privacy.

B. National law and framework

5. Australia is a federal constitutional monarchy. Government in Australia consists of the federal Government, state and territory governments and local government bodies. Australia has a fragmented legal framework derived from the Constitution of Australia, state constitutions and the common law, which is protected by judicial and parliamentary review.

6. The Constitution confers power on the federal Parliament to make laws only on certain subject matters. The six Australian states are formally recognized by the Constitution and, subject to the Constitution, have powers to pass laws on most subject matters. In the event of inconsistency between a law of the Commonwealth and a law of a state, the Commonwealth law prevails. The two self-governing territories have more limited legal independence and the federal Parliament can override laws in the territories.

7. On 30 May 2024, the federal Parliamentary Joint Committee on Human Rights published its report[2] on its inquiry into the country's human rights framework and recommended that the Government re-establish and significantly improve the framework, including through the establishment of a human rights act, and outlined an example of the necessary legislation. Moreover, the Committee acknowledged that protection of privacy in the digital age was a significant human rights problem in Australia.[3]

8. The Australian Human Rights Commission is responsible for monitoring the country's performance in meeting its international human rights obligations and welcomed the report of the Parliamentary Joint Committee on Human Rights, which builds on the Commission's recommendations regarding a national human rights framework.[4]

9. While some states in Australia have a human rights act, the country lacks a human rights act at the national level. The Australian Human Rights Commission has called for a federal human rights act to better explain and solidify human rights, including the right to privacy, and enable citizens to have a clear path to file grievances and protect against arbitrary or unfair decision-making due to the inconsistent application that can result from different outcomes at the state or territory level.

III. Privacy Act

10. The Privacy Act 1988 gives effect to the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Organisation for Economic Co-operation and Development, and the obligations arising under article 17 of the International Covenant on Civil and Political Rights.[5] The Privacy Act is a federal law that does not cover local, state or territory government agencies, except the Norfolk Island administration. Most Australian states and territories have equivalent legislation that covers their public sector agencies.

11. The Privacy Act regulates the protection, handling, storage, use and disclosure of individuals' personal information.[6] The Act's purpose is to protect an individual's personal information from "arbitrary interference" and from "harm stemming from the misuse of their personal information".[7] It aims to balance the protection of the right to privacy by assessing whether the entity's effect on the individual's privacy is "necessary, reasonable and proportionate to achieving [its] legitimate functions and … public interests".[8]

[2] Parliamentary Joint Committee on Human Rights, *Inquiry into Australia's Human Rights Framework* (2024).
[3] Ibid., p. 297.
[4] See https://humanrights.gov.au/sites/default/files/2311_freeequal_finalreport_1_1.pdf.
[5] See https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act.
[6] See https://www.ag.gov.au/rights-and-protections/privacy#:~:text=The%20Privacy%20Act%201988%20.
[7] Office of the Australian Information Commissioner, *Privacy Act Review – Issues Paper* (2020), p. 21.
[8] Ibid., p. 22.

12. The Privacy Act was significantly amended in 2014 and 2017. The 2014 reforms introduced the Australian Privacy Principles (or APP),[9] which are the key feature of the current Act. The 13 Australian Privacy Principles regulate the handling of personal information by federal Government agencies and some private sector organizations. The 2017 reforms to the Privacy Act introduced a notifiable data breaches scheme for organizations and agencies covered by the Privacy Act. That scheme mandates notification to the privacy regulator and the individual concerned when an entity that is operating according to the Australian Privacy Principles experiences a data breach of personal information that may cause serious harm to the individual.[10]

IV. Privacy Act review process

13. The impetus for legislative reform stems from recommendations made by the Australian Competition and Consumer Commission in its final report published in 2019 for the Digital Platforms Inquiry.[11] In October 2020, the Government initiated the Privacy Act review. On 16 February 2023, the Attorney-General's Department, tasked with the implementation of the Government's response to the Privacy Act review, published the Privacy Act review report and made 116 proposals, the culmination of extensive public consultations with federal entities, state and territory government departments, the private sector and privacy regulators. On 28 September 2023, the Government published its response to the Privacy Act review report[12] and "agreed" with 38 of the 116 proposed changes in the report and "agreed in principle" to another 68 to better protect citizens' privacy.

14. The obligation to consider, upfront, what personal information it wishes to collect, whether it is entitled to do so under the Privacy Principles and the Privacy Act and if there is a less intrusive way, in relation to privacy, to meet its objectives (i.e. not collecting personal information or collecting less of it) will substantially shift business to more of a "privacy by design" approach.

15. Unlike its European counterparts, the Privacy Act does not distinguish between the categories of "data processors" and "data controllers". According to section 6 (1) of the Privacy Act, "APP entity means an agency or organisation". However, in response to the recent Privacy Act review report, the Government has agreed, in principle, to introduce the concepts of "controller" and "processor" used in the General Data Protection Regulation, which would increase the oversight powers and responsibilities of these key roles to more robustly protect the right to privacy, "bring Australia into line with other jurisdictions" and simplify privacy obligations.[13]

16. The Special Rapporteur welcomes the enormous task carried by the Government to conduct a major review of the Privacy Act. Having consulted with all interlocutors, it appears that the initiative is more reactive than proactive and the implementation of the recommendations that came out of the review process have not yet all been implemented to adequately address the gaps in the privacy framework.

17. On 29 November 2024, Parliament passed the Privacy and Other Legislation Amendment Act 2024.[14] which represents the first tranche of reforms following the comprehensive review of the Privacy Act. It implements 23 key changes from the recommendations made in the Privacy Act review report. Below is an overview of its key elements:

(a) Introduction of a statutory tort for serious invasions of privacy, allowing individuals to seek redress directly for intentional or reckless breaches;

[9] See https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf.
[10] Attorney-General's Department, *Privacy Act Review Report 2022* (2022).
[11] See https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report.
[12] Government of Australia, "Government response: Privacy Act review report" (2023).
[13] Ibid., p. 15.
[14] See https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7249.

(b) Transparency and enforcement enhancements: clarifies key definitions and concepts in the Privacy Act and in the Australian Privacy Principles and increases funding and strengthens the powers of the Office of the Australian Information Commissioner (including the Privacy Commissioner) and the Federal Court regarding enforcement and public inquiries, along with tiered civil penalties for privacy violations;

(c) Automated decision-making: requires businesses to increase transparency and disclose details in their privacy policies about the use of personal information in automated decision-making that significantly affects the rights or interests of individuals;

(d) Children's online privacy code: mandates the Office of the Australian Information Commissioner (specifically, the Australian Information Commissioner) to develop a code to protect minors, which could impose additional requirements on APP entities that are providers of a social media service, relevant electronic service or designated Internet service, in situations in which the service is likely to be accessed by children;

(e) Criminalization of doxxing: amends the Criminal Code Act 1995, to include criminal offences for the harmful online disclosure of personal information in a manner that would be menacing or harassing;

(f) Cross-border data flow mechanism: introduces a mechanism to increase certainty and efficiency for individuals and businesses to further facilitate international data-sharing or personal information with other jurisdictions.

18. The exemption of small businesses from the Privacy Act remains unchanged and has been criticized.[15] Those exemptions have been criticized for not requiring privacy compliance for large portions of the private sector and are "the key factor behind Australia being considered 'not adequate' for the purposes of cross-border disclosure out of the EU pursuant to the EU General Data Protection Regulation (GDPR)".[16] However, the Government has agreed in principle to amend the exemption.[17]

19. Overall, the first tranche of reforms are an important and much needed step in modernizing the privacy framework and an important and long overdue first step. The Government has committed to further reforms identified in the numerous recommendations raised in the Privacy Act review report, with the implementation of a second tranche, although the timeline remains unclear.

A. Office of the Australian Information Commissioner and the Australian Competition and Consumer Commission

20. The Office of the Australian Information Commissioner is the federal privacy regulator in Australia. The Office was established as an independent regulator in 2010 and operates under a three-commissioner model. The Office consists, in addition to other staff, of three statutory office holders: the Australian Information Commissioner (as head of the Office), the Privacy Commissioner and the Freedom of Information Commissioner.

21. The purpose of the Office of the Australian Information Commissioner is promoting and protecting privacy and access to information. The Office's enforceable powers include ensuring entities (Government agencies and businesses) conform with the Privacy Act by conducting assessments, investigating breaches of the Australian Privacy Principles, handling privacy complaints, seeking civil penalties and advising the public, organizations and agencies.[18]

22. The Australian Competition and Consumer Commission is another independent federal agency and a powerful regulator of digital platforms and data at the intersection between privacy, competition and consumer protection. For the past five years, the

[15] Attorney-General's Department, *Privacy Act Review Report 2022*, pp. 52–63.

[16] See https://www.privacyworld.blog/2024/12/first-tranche-of-reforms-to-australian-privacy-law-passed-with-amendments.

[17] Government of Australia, "Government response: Privacy Act review report", p. 6.

[18] See https://www.oaic.gov.au/about-the-OAIC/what-we-do.

Commission has conducted an inquiry into markets for the supply of digital platform services,[19] which is putting privacy in the public spotlight. In the eighth interim report,[20] which focused on the collection and use of consumer data by data brokers, the Commission found that Australians were unaware of how much of their personal data was being collected due to ambiguous privacy policies.

23. The Special Rapporteur noted that there appears to be some overlap between the mandates of the Australian Competition and Consumer Commission and the Office of the Australian Information Commissioner. The Commission has shown a willingness to act on consumer matters that relate to privacy, by conducting investigations and proceedings under consumer law against companies for misleading and deceptive conduct concerning the collection, use and disclosure of personal information. However, the Office has gained increased recognition for its role regarding the protection of privacy due to its strengthened regulatory powers and willingness to take on a more robust role in enforcement.

B. State and territory privacy legislation and regulators

24. Most states and territories in Australia have their own data protection and privacy legislation applicable to their own government agencies and some private businesses. However, in practice, it is a piecemeal system that requires a more comprehensive and updated approach. The Privacy Act review process is set to reform and update the existing federal framework. Thus, implementing those recommendations will not affect state and territory laws or responsibilities, or the structure of Australian privacy frameworks. However, the Privacy Act review has also recommended the establishment of a Commonwealth, state and territory working group to harmonize privacy laws, focusing on key issues, which is under consideration by the Government.

V. Protection of personal data

25. As people's lives are increasingly moving to the online space "privacy is fast becoming one of the most casually and frequently breached, but immeasurably important, human rights … with breaches of privacy … leading to a more dangerous world … or identity theft".[21]

26. The Special Rapporteur heard complaints of stockpiling of personal data that was sold and used to analyse, manipulate, profile and conduct electronic surveillance of data subjects without their knowledge. Australia has a well-documented history of high-profile data breaches,[22] which triggered real concerns about the capability of both the Government and the private sector to safely store and manage personal data.

27. The Government's response has been very public in an effort to restore confidence and increase transparency as breaches led to the exposure of a total of 416 million personal records in Australia, including 97 million passwords,[23] which resulted in large numbers of individuals being at risk of serious cyberthreats, such as identity theft.

28. The National Identity and Cyber Support Service of Australia and New Zealand plays a key role in supporting individuals, small businesses and vulnerable or remote communities that have suffered data breaches due to cybercrimes, scams and identity theft; it helps them to access remedies to minimize harm suffered by such privacy violations.

[19] See https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25.

[20] See https://www.accc.gov.au/about-us/publications/serial-publications/digital-platform-services-inquiry-2020-25-reports/digital-platform-services-inquiry-interim-report-march-2024 and https://www.abc.net.au/news/2024-05-21/accc-digital-services-data-report/103872726.

[21] Parliamentary Joint Committee on Human Rights, *Inquiry into Australia's Human Rights Framework*, p. 46.

[22] See https://www.insurancebusinessmag.com/au/news/cyber/data-breach-tsunami-hits-australia-486903.aspx.

[23] Ibid.

29. The Digital ID Act 2024[24] entered into force in December 2024 to facilitate the voluntary, convenient, secure and inclusive verification of identity online for transactions with Government and businesses. The Act will be jointly regulated by the Office of the Australian Information Commissioner in relation to the privacy aspects thereof and the Australian Competition and Consumer Commission will monitor and enforce the other aspects.

A. Health data

30. Data containing identifiable information about a person must comply with the Privacy Act, which applies to all private sector healthcare providers throughout Australia. Most Australian states and territories have equivalent legislation, which covers their public sector agencies regarding health data, however, it is a complex and patchwork system. The Special Rapporteur noted the need for greater cooperation regarding the sharing of information across internal state/territory borders. For example, the challenges regarding individuals living in one state and going to school/work in another state when accessing health services (and ensuring privacy of their medical records) due to decentralization and different governing frameworks.

31. The Special Rapporteur noted that state and territory privacy commissioners and information commissioners met regularly to discuss challenges and trends with the aim of trying to ensure consistency in application, interpretation and approach but a more systemic approach, with more stringent safeguards, is needed to ensure that sensitive health data can be shared across various jurisdictions in a safe and private manner.

32. The Australian Digital Health Agency advised that the "My Health Record" system had been created for the purpose of facilitating safe and private sharing of health information by healthcare practitioners across jurisdictions. If the Health Legislation Amendment (Modernising My Health Record – Sharing by Default) Act 2025 were fully implemented, it would hopefully improve that sharing process.

B. Mandatory SIM card registration

33. SIM card registration is mandated in Australia, where the "capture and store" approach is adopted, meaning mobile network operators and all carriage service providers that supply prepaid mobile carriage services must obtain and store, generally for two years after the closure of the account, certain personal information about SIM card owners (name, date of birth and records to demonstrate compliance with the verification requirements) (Telecommunications (Interception and Access) Act 1979, sect. 187C (1) (a)). Law enforcement agencies may have access to users' information to investigate serious and organized crimes.[25]

34. The Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 requires mobile service providers to verify a customer's identity at the point of purchasing or activating a mobile prepaid service.[26] It is understood that in Australia most telecommunication providers supplying services verify the identity of customers who are service activators. Information obtained from those customers includes the service activator's name and date of birth. If the service activator is activating the service on behalf of an entity, the name of the entity and business address, otherwise their residential address, are required. Telecommunication providers must verify identity using an approved method that sets out rules that must be followed, such as a government online verification system, a whitelisted email address, a financial transaction, an existing prepaid or postpaid account or a visual identity check. Telecommunication providers are also required

[24] See https://www.accc.gov.au/by-industry/digital-platforms-and-services/digital-identity.

[25] See https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Former_Committees/acc/completed_inquiries/2004-07/organised_crime/report/c07.

[26] Sect. 4.2.

to record sufficient information to demonstrate that they have complied with the Prepaid Determination.[27]

35. In 2022, the Government introduced new regulations utilizing multi-factor authentication measures to impede fraud relating to SIM-swap practices; as, although scammers may steal a proof of identity, "they [would] still need to obtain and use the other proofs of identity to access your account".[28]

VI. Emerging technologies

A. Biometric data

36. Under the Privacy Act, biometric information (electronic copy of features, including face, fingerprints, iris, palm, signature and voice) is classified as "sensitive information" and specific obligations are imposed on the collection of such sensitive information. Organizations or agencies that collect your biometric information must first ask for consent, with exceptions for those that lack capacity whereby another individual may consent for them.[29]

37. The Government's response to the Privacy Act review report supports the introduction of stricter measures regarding the use of biometric surveillance technologies by regulated entities. The Government has agreed in principle that all entities that collect biometric information (regardless of size) should be required to comply with the controls in the Privacy Act.

38. The Digital ID Act does authorize certain entities to collect, use and disclose biometric information in specific circumstances and obliges them (with limited exceptions) to obtain the express consent of the individual for the collection, use and disclosure of such information.

B. Facial recognition technology

39. The Special Rapporteur learned that facial recognition technology was used by Government and business and in various public locations, such as retail outlets and sport and entertainment venues, and that it represented one of the biggest potential privacy risks faced by citizens.

40. Australian society does appear to support use of facial recognition technology for some services, including the new Digital ID system, which will enable citizens to prove their identity when accessing government and private services. That is a welcome development provided the key requirements of adequate notification and consent are deployed to protect privacy when using that technology.

41. Based on a recent survey,[30] 75 per cent of citizens support the use of facial recognition technology as a surveillance tool for identifying criminal suspects. However, a majority (60 per cent) of survey respondents did not support its use in the workplace for tracking the location of workers. Nor did they support its use for tracking and targeting shoppers.

42. The Special Rapporteur is concerned about the increased practice of entities' requiring biometric information to access services. On 19 November 2024, the Privacy Commissioner

[27] Sects. 1.8, 4.3–4.5 and 6.1.

[28] See https://www.biometricupdate.com/202204/australia-considers-following-african-countries-in-biometric-sim-registration-to-curb-crime.

[29] See https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning#:~:text=Under%20the%20Privacy%20Act%201988,high%20level%20of%20privacy%20protection.

[30] See https://theconversation.com/australians-like-facial-recognition-for-id-but-dont-want-it-used-for-surveillance-new-survey-shows-235530#:~:text=Automated%20facial%20recognition%20is%20becoming,parliament%20earlier%20in%20the%20year.

issued findings in a case concerning Bunnings Group Limited and found that citizens' privacy had been violated by the retail company's practice of collecting personal and sensitive information through a facial recognition technology system due to a lack of proportionality (intrusive nature of gathering biometric information) and transparency (lack of consent to collect sensitive facial imaging). Between November 2018 and 2021, closed-circuit television used facial recognition technology to capture the faces of every person entering 63 stores in Victoria and New South Wales as a cost effective measure to try to address unlawful activity.[31]

43. The Special Rapporteur welcomed the decision of the Privacy Commissioner, namely that the facial recognition technology in that case violated the Privacy Act as Bunnings had failed to take reasonable steps to implement adequate procedures and safeguards. The Special Rapporteur cautioned that emerging technologies raise various ethical considerations and expressed concern about the use of facial recognition technology in criminal investigations without adequate safeguards.

44. In response to the Bunnings case, the Office of the Australian Information Commissioner issued "Facial recognition technology: a guide to assessing the privacy risks"[32] for private sector organizations that are considering using facial recognition technology in retail settings. The guide does not cover all privacy issues and obligations in relation to the use of facial recognition technology, although it provides information about key principles captured under the Australian Privacy Principles (1, 3, 5 and 10).

45. As legislation regulating facial recognition technology is lacking, greater regulation is needed to protect the right to privacy. The Government has agreed in principle that non-government entities should be required to complete a privacy impact assessment for high-risk activities prior to those activities taking place, in conjunction with the requirement for more privacy enhanced risk assessments for facial recognition technology and the use of biometric information.[33]

46. The Australian Human Rights Commission has raised concerns regarding facial recognition technology and lack of accuracy and fairness relating to racial and gender bias. The Special Rapporteur shares the concerns expressed by civil society that already marginalized and vulnerable groups are likely subject to greater surveillance than the general population and facial recognition technology could result in overpolicing in these communities. The result is that specific sectors of society (Indigenous people and LGBTQI+ persons) experience a further erosion of their trust in institutions (law enforcement and the courts) responsible for enforcing legal safeguards and oversight against arbitrary interference in the right to privacy.

C. Artificial intelligence

47. In January 2024, the Government released its interim response to the "Safe and responsible AI consultation",[34] which provides a road map outlined by key interlocutors in industry, academia and civil society to guide the Government's development and deployment of artificial intelligence in a responsible manner, including safeguarding the right to privacy.

48. The Special Rapporteur emphasizes that it is impossible for law to keep up with technological advances as there will always be normative gaps. The law by nature is retroactive as it is only implemented once there is a problem. In an increasing digitalized age, artificial intelligence, which is particularly invasive, will continue to evolve rapidly.

[31] See https://www.oaic.gov.au/news/media-centre/bunnings-breached-australians-privacy-with-facial-recognition-tool.

[32] See https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks.

[33] Australian Human Rights Commission, *Safeguarding the Right to Privacy in Australia* (Sydney, 2023), p. 15.

[34] See https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/safe-and-responsible-ai-in-australia-governments-interim-response.pdf.

Innovation should be embraced, but it must have a human rights-based approach to protect privacy and respect the principle of do no harm. The Office of the Australian Information Commissioner has issued guidance on artificial intelligence to help businesses comply with their privacy obligations.[35]

49. The Special Rapporteur shared concerns raised in the report of the Parliamentary Joint Committee on Human Rights regarding the implications of neurotechnology (which allows the human brain to connect directly to digital networks through processes and devices that permit the neural processes to be accessed, monitored and manipulated) and the need for regulation regarding the collection, storage and sale of neural data, and protection of thoughts against disclosure.[36] Neurorights should be recognized to protect against the infringement of cognitive liberty, freedom of thought, personality and free will, which are essential elements of an individual's mental privacy.

50. The new statutory tort for serious invasions of privacy may enable citizens to seek a remedy before the court, should any of the emerging technologies be misused in a discriminatory or unauthorized manner.

VII. Cybersecurity and cybercrime

51. The Government introduced the 2023–2030 Australian Cyber Security Strategy, which is aimed at improving cybersecurity, upgrading data security settings, managing cyberrisks and better supporting citizens and Australian businesses to manage the cyberenvironment.

52. On 29 November 2024, the Cyber Security Act 2024 received royal assent.[37] The new Act strengthens privacy safeguards for individuals, businesses and critical infrastructure, enhancing the resilience of Australia in relation to cyberthreats. The Act introduces a mandatory ransomware and cyberextortion reporting obligation for certain businesses to report ransom payments. It also introduces a limited use obligation for the National Cyber Security Coordinator to encourage industry engagement with the Government following cyberincidents. Furthermore, the Act mandates minimum cybersecurity standards for smart devices and introduces a new Cyber Incident Review Board to respond to emerging challenges in a rapidly evolving digital environment.

53. The National Office of Cyber Security leads the coordination of national cybersecurity policy, preparedness efforts and responses to major cyberincidents. The Office of the Australian Information Commissioner is responsible for overseeing and enforcing the mandatory Notifiable Data Breaches scheme (in which a cyberincident includes personal information)

54. The mandate of the eSafety Commissioner is to safeguard citizens from online harms and promote safer, more positive online experiences. The Commissioner conducts research, promotes online safety awareness, provides programmes to prevent online harms and acts as a safety net across four areas: adult cyberabuse; cyberbullying of children; image-based abuse; and illegal and restricted content. In November 2023, the Government ordered an independent statutory review of the Online Safety Act 2021 and, on 31 October 2024, it received a final report,[38] which was published on 4 February 2025. The report contained recommendations on changing how the eSafety Commissioner regulated industry codes, including on illegal and restricted content, such as that pertaining to terrorism, violent and child sexual abuse. The Government has yet not tabled a response to the report.

[35] See https://www.oaic.gov.au/news/media-centre/new-ai-guidance-makes-privacy-compliance-easier-for-business.

[36] Parliamentary Joint Committee on Human Rights, *Inquiry into Australia's Human Rights Framework*.

[37] See https://www.wottonkearney.com/breaking-down-the-cyber-security-act-2024-and-amendments-to-the-soci-act.

[38] See https://minister.infrastructure.gov.au/rowland/media-release/government-welcomes-report-australias-online-safety-laws.

VIII. Law enforcement and intelligence agencies

55. The powers to execute a search warrant (to enter premises, collect forensic evidence etc.), as contained in division 2 of the Crimes Act 1914,[39] are executed by a law enforcement officer in the context of criminal investigation in accordance with the safeguards of the Privacy Act 1988, the Australian Federal Police Act 1979 and the Crimes Act 1914.[40] For other investigative techniques, Australia has a complex legal framework governing surveillance and national security and the Government continues to strive to ensure an appropriate balance between the powers of law enforcement and intelligence services and providing effective safeguards and robust oversight.

56. The Telecommunications (Interception and Access) Act 1979 governs the interception of communications and access to stored communications (email, text and voice messages) in relation to Commonwealth, state and territory criminal investigations, and matters of national security. The Surveillance Devices Act 2004 regulates the use of surveillance devices, such as listening devices and optical surveillance, in relation to Commonwealth criminal investigations, and state and territory criminal investigations that have a federal aspect. Each state and territory has implemented its own surveillance devices laws as part of a national model laws framework governing the use of surveillance devices within their jurisdiction, and for the purposes of their respective criminal investigations.

57. There are legal safeguards in conducting such privacy-intrusive activities. Law enforcement and intelligence agencies must obtain a warrant or authorization, under the Telecommunications (Interception and Access) Act or the Surveillance Devices Act, issued by a judge or other independent authorized person, based on the strict criteria of necessity and proportionality, to exercise those powers.[41]

58. The Assistance and Access Act 2018 strengthened the ability of law enforcement and security agencies, under warrant, to collect evidence from electronic devices. Telecommunications service providers are required to retain metadata for a minimum period, which can be accessed by law enforcement agencies and the Australian Security Intelligence Organisation.

59. The Surveillance Legislation Amendment (Identify and Disrupt) Act 2021[42] introduced three new investigative powers[43] for the Australian Federal Police and the Australian Criminal Intelligence Commission to respond to cyber-enabled crime in the digital era:

(a) Data disruption warrants allow the disruption of data through modification and deletion of data to frustrate the commission of serious offences, such as the distribution of child abuse material;

(b) Network activity warrants allow the collection of intelligence on criminal networks operating online;

(c) Account takeover warrants allow control of a person's online account to gather evidence about criminal activity to further a criminal investigation.

60. There are various oversight mechanisms, including parliamentary committees, independent reviewers and the Commonwealth Ombudsman,[44] to ensure that surveillance powers are used lawfully and appropriately. The Commonwealth Ombudsman is the oversight authority of the Australian Federal Police. The use of electronic surveillance

[39] See https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ca191482/s3f.html.

[40] See https://www.afp.gov.au/our-services/national-policing-services/search-warrants.

[41] See https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-limitations-safeguards.

[42] See https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021.

[43] See https://www.ag.gov.au/crime/publications/factsheets-warrants-under-surveillance-legislation-amendment-identify-and-disrupt-act-2021.

[44] See https://www.ombudsman.gov.au/industry-and-agency-oversight/law-enforcement-integrity-oversight.

powers by the Australian Criminal Intelligence Commission are subject to strict record-keeping regarding the use and disclosure of information collected pursuant to warrants and destruction requirements. The Inspector-General of Intelligence and Security[45] oversees network activity warrants, given their nature as an intelligence collection tool. Furthermore, judicial review by the courts is available under the Judiciary Act 1903.

61. In December 2019, the Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review) recommended repealing and replacing the Telecommunications (Interception and Access) Act, the Surveillance Devices Act and parts of the Australian Security Intelligence Organisation Act 1979 with a single tech-neutral act (recommendation 75)[46] that is fit for purpose in the digital age.

62. In July 2022, an inter-agency task force within the Attorney-General's Department succeeded the Department of Home Affairs to progress those major reforms on electronic surveillance laws.[47] The purpose of the review was to formulate laws that protect privacy, promote transparency and offer clarity to the agencies and oversight bodies as existing laws were outdated, complex and confusing, in part due to the patchwork of overlapping laws, as a result of numerous amendments spanning several decades.

63. The Government has implemented several other recommendations from the Richardson Review, including through the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023.[48]

IX. Remedies

64. Prevention is the best remedy for a breach of privacy because once a violation has occurred it is very difficult to right the harm as it cannot be reversed once information is in the public domain. It is also very important to work on improved access to a remedy (administrative and judicial) and the redress (compensation etc.), which were the focus of a thematic report by the Special Rapporteur, in which she conducted a comparative analysis of legal safeguards across various legal systems.[49] In Australia, the Privacy Commissioner may require an entity under investigation to engage an independent adviser to review the situation and provide a copy of the review to the Commissioner. The Privacy Commissioner may also require the entity to prepare and publish a statement about its conduct.[50] There is also the possibility of referring the matter to an alternative dispute resolution mechanism as a preliminary measure.[51]

65. The Special Rapporteur welcomed the introduction of a statutory tort on serious invasion of privacy, passed by Parliament in the first tranche of reforms to the Privacy Act and scheduled to come into effect on 10 June 2025.[52] The statutory tort will apply to a broader group of entities and individuals than those regulated by the Act and will include invasions of physical privacy. In that way, the tort will expand the implementation of the right to privacy.

[45] See https://www.igis.gov.au/sites/default/files/2024-10/IGIS%20Annual%20Report%202023-24.pdf.

[46] See https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework.

[47] See https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework.

[48] See https://www.ag.gov.au/system/files/2020-12/Government-response-to-the-Comprehensive-Review-of-the-Legal-Framework-of-the-National-Intelligence-Community_1.PDF.

[49] A/HRC/55/46.

[50] Ibid., para. 105.

[51] Ibid., para. 98. For more details about the remedies available in Australia, see tables 3, 4 and 5 of the report.

[52] See https://www.tglaw.com.au/insights/six-month-countdown-to-new-statutory-tort-of-serious-invasions-of-privacy#:~:text=New%20legislation%20introducing%20a%20statutory,Parliament%20and%20given%20Royal%20Assent.&text=The%20cause%20of%20action%20will,as%20the%20legislation%20is%20tested.

X. Gender

66. The right to the free development of personality is protected under articles 22 and 29 of the Universal Declaration of Human Rights. Moreover, the Human Rights Council, in its resolution 34/7, makes the explicit link that the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity.

67. The Special Rapporteur reminds the Government of the view expressed by the Human Rights Committee, namely that the right to privacy covers gender identity.[53] The Special Rapporteur heard testimonies from advocates who are trying to ensure that individuals have the right to keep private information about their gender identity at birth and any legal changes to their name or medical interventions (and any health records). Those issues require urgent attention and equal protection due to the jurisdictional challenges at the federal, state and territory levels.

68. The National Plan to End Violence against Women and Children 2022–2032 is the overarching national policy framework intended to guide actions towards ending violence against women and children, which must be urgently prioritized due to the increasing levels of domestic violence in Australia. The Special Rapporteur learned that there was a lack of safe private space for those who wished to leave violent relationships and that, among others, the frequent use of mobile applications to stalk a partner's movements and control finances had only further increased the risks, in particular, to women and children.

69. Homosexuality was decriminalized across all states and territories in Australia by the 1990s, with the decriminalization of homosexuality in Tasmania following the Views of the Human Rights Committee in *Toonen v. Australia*, in which it found a violation of the right to privacy under article 17 of the International Covenant on Civil and Political Rights.[54] To implement the international obligations of Australia under article 17 of the Covenant, the federal Government passed the Human Rights (Sexual Conduct) Act 1994, which holds that sexual conduct between consenting adults in private shall not be subject, by or under any law of the Commonwealth, a state, or a territory, to any arbitrary interference with privacy.[55]

70. The Special Rapporteur noted that one of the issues that is currently the focus of LGBTQI+ rights activism in Australia is the increasing challenge to access to formal identity documents that match a person's gender identity.

71. The Office of the Victorian Information Commissioner published a guide on LGBTQI+ privacy rights outlining how Victorian privacy law may apply to LGBTQI+ communities.[56] The state's Privacy and Data Protection Act 2014 gives protection to LGBTQI+ communities by classifying information about sexuality as "sensitive information". Although gender identity and sex are not classified as sensitive information, the Office of the Victorian Information Commissioner recognizes that such information is delicate and must be treated with care.

72. In the State of Western Australia, the definition of "sensitive personal information" in its Privacy and Responsible Information Sharing Act 2024 expressly includes gender identity in situations in which individuals' gender identity does not correspond with their designated sex at birth. That helps to ensure additional protections for that category of information.

XI. Children and digital space

73. The Convention on the Rights of the Child enshrines the right to privacy in article 16; the Privacy Act contains no special or additional protections for children as it protects all individuals' personal information irrespective of their age.[57] As a result, the organization or

[53] See CCPR/C/119/D/2172/2012.
[54] Human Rights Committee, communication No. 488/1992, *Toonen v. Australia*.
[55] Sect. 4. See https://www.legislation.gov.au/C2004A04852/latest/text.
[56] See https://ovic.vic.gov.au/privacy/for-the-public/lgbtiq-privacy-rights.
[57] See https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/consent-to-the-handling-of-personal-information#AlertConsent.

agency handling the personal information of individuals under the age of 18 must decide if the child (under 18) providing information has the capacity to do so on a case-by-case basis. However, as noted by the Office of the Australian Information Commissioner, if it is not practical for an organization or agency to assess capacity on a case-by-case basis, as a general rule, an organization or agency may assume an individual over the age of 15 has capacity, unless it is unsure.[58] The use of "the child's best interests" should be the central approach in privacy protection and data processing.

74. In 2022, the Government held an inquiry into social media and online safety and sought submissions from civil society and advocacy groups. The Special Rapporteur participated in a round table hosted by the Victorian Equal Opportunity and Human Rights Commission on ongoing challenges to protect children's privacy in the digital space. First, the sophisticated attention-harnessing techniques underpinning the business models of technology companies heavily influence children's experiences online, in particular, because their brain, social development, identity and cognitive ability are all still forming.[59] Second, as children's privacy is not adequately protected when using websites and playing games online,[60] even for education use, the scale and scope of technological networking pose a high risk of exploitation and a potential gateway to online abuse and other online harms.[61] The state-level governments of New South Wales and Victoria have opened investigations into protecting children's use of online learning platforms[62] as 4 million students (during the coronavirus disease (COVID-19) lockdown) were at risk of unprecedented tracking and surveillance during remote learning as corporations exploited their access to children.[63]

75. Children have their own perspective regarding privacy – which has been captured by the Australian Child Rights Taskforce, a body that prioritizes the best interests of the child, which noted that older children can have a more sophisticated understanding about privacy in the digital context and an increasing awareness of how frequently the associated right is violated.

76. The Special Rapporteur noted, therefore, that it was essential for children, starting from a very young age, to develop their digital literacy and understanding of informed consent regarding the collection and use of data to ensure an online environment that balances increasing autonomy with safety.

77. The Special Rapporteur welcomed the introduction, in December 2024, of the requirement to develop a children's online privacy code, as recommended in the Privacy Act review, as previously there were no specific laws to enhance online protections to more robustly protect children's data privacy.

78. The Privacy and Other Legislation Amendment Act has addressed the lack of protections specific to children and mandated the Information Commissioner to develop a children's online privacy code to apply to online services likely to be accessed by children under 18.

79. In its response to the Privacy Act review, the Government agreed in principle to prohibit the direct marketing of products to children for advertising purposes unless the prohibition was contrary to the best interests of the child, to ban the trading of children's personal information and to ensure that online service providers prioritized the best interests

[58] See https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people#:~:text=The%20Privacy%20Act%201988%20protects,must%20have%20capacity%20to%20consent.

[59] See https://www.savethechildren.org.au/getmedia/f62be1cd-a8aa-4fbc-b990-4ab01ef35e55/inquiry-into-social-media-and-online-safety.pdf.aspx.

[60] See https://childrenandmedia.org.au/assets/files/resources/ReportACCMPrivacyResearchProject.pdf.

[61] See https://www.alannahandmadeline.org.au/what-we-do/advocacy/digital-rights.

[62] See https://www.hrw.org/news/2023/02/14/some-governments-companies-take-steps-protect-children.

[63] See https://www.abc.net.au/news/2022-05-25/investigation-reveals-educational-tech-tracking-children-data/101091808.

of the child when handling children's data.[64] Implementation of the children's online privacy code will be under the authority of the Information Commissioner.

80. On 29 November 2024, Parliament passed the Online Safety Amendment (Social Media Minimum Age) Act 2024,[65] which establishes a minimum age (16 years) for social media use and an obligation on providers to take reasonable steps to prevent age-restricted users having accounts with age-restricted social media platforms.[66] It will result in Australia having very strict age restrictions (as it does not include exemptions for existing users or those with parental consent).

81. The legislation specifies that the Minister may make legislative rules specifying services that are or are not covered by the Act, which could include Snapchat, TikTok, Facebook, Instagram and X. The eSafety Commissioner will be responsible for enforcing the provisions that services must take "reasonable steps" to ensure age-restricted users do not have accounts with age-restricted social media platforms. The explanatory memorandum to the associated bill sets out that, at a minimum, that should include some form of age assurance (which is broader than age verification) but what these reasonable steps may be are "to be determined objectively, having regard to the suite of methods available, their relative efficacy, costs associated with their implementation, and data and privacy implications on users, amongst other things". The eSafety Commissioner will issue guidance in 2025 about what constitutes reasonable steps, informed as well by the findings of the age assurance technology trial. The onus will be on the social media platforms to add those processes themselves and technology companies could be fined up to 50 million Australian dollars if they do not comply.

XII. Digital literacy and vulnerable groups

82. The Government acknowledged the challenges of the principle of "leave no one behind" in the digital age and the need to ensure that awareness, education, transparency, oversight and accountability measures and redress were in place to protect the safety of those with specific vulnerabilities and a higher risk of harm, including children, older persons and rural populations, Indigenous people, linguistically diverse and culturally diverse persons, neurodivergent persons, persons with disabilities, LGBTQI+ persons, in relation to privacy infringements in the online context.

83. There are Commissioners in the Australian Human Rights Commission who advocate for various groups, including the National Children's Commissioner and the Age Discrimination Commissioner, but there is a need for greater protection for privacy rights to ensure that concepts of consent and personal autonomy online are strengthened to prevent online abuse, including sexual exploitation, harassment, bullying, mental distress and financial manipulation.

84. The Government has acknowledged the historic institutionalized and systemic marginalization and discrimination of Indigenous Peoples, including with respect to their right to privacy. The Special Rapporteur noted some initial steps towards accountability, such as the Yoorrook Justice Commission, the first formal truth-telling process into injustices experienced by First Peoples in the State of Victoria, which held hearings at the outset on how to safeguard the information and data gathered during the inquiry regarding Indigenous Peoples.

85. The National Indigenous Australians Agency published a Framework for Governance of Indigenous Data,[67] co-designed with Indigenous communities, to provide guidance to the Australian Public Service on how to provide Aboriginal and Torres Strait Islander peoples with greater agency over how their data are governed. Research has also been carried out on

[64] See https://www.alannahandmadeline.org.au/news/a-childrens-online-privacy-code-what-could-it-mean-for-parents-and-caregivers.
[65] See https://www.legislation.gov.au/C2024A00127/asmade/text.
[66] See https://www.bbc.com/news/articles/c89vjj0lxx9o.
[67] See https://www.niaa.gov.au/resource-centre/framework-governance-indigenous-data.

Indigenous data sovereignty regarding ownership and control of data by Indigenous communities.[68]

86. The Office of the Victorian Information Commissioner, in its report on Understanding Culturally Diverse Privacy, Aboriginal and Torres Strait Islander peoples' perspectives,[69] discussed the concept of privacy as a group right, and among its findings were Aboriginal concerns about the collection of personal information, particularly the sharing of information about Elders or peers, and historical and other factors, which may result in distrust of organizations, and fears of information on racial or ethnic origin being collected and used for negative purposes.

87. It is important to acknowledge that Indigenous Peoples have a unique and collective view of privacy that prohibits the sharing of the voices or images of the deceased. In addition, women and men keep private certain traditional ceremonial rites from the other gender. The Australian Law Reform Commission has also considered "privacy protocols for Indigenous peoples"[70] as the National Identity and Cyber Support Service of Australia and New Zealand has highlighted the lack of culturally appropriate accessibility to express privacy infringements as Aboriginal languages do not have words for identity credentials, identity theft, scams and cybercrime.[71]

88. The Special Rapporteur also noted the specific vulnerabilities of Indigenous children to protect their online and offline privacy as they often lack access to private home settings and are placed in residential homes in which there is a higher risk of sexual exploitation.

XIII. Conclusions and recommendations

89. **The Special Rapporteur welcomes the comprehensive reforms proposed by the Privacy Act review and the commitment displayed by the Government to embark on a major upgrade of privacy protections. After many years of deliberation, the first tranche of reforms were passed in November 2024. However, numerous legislative and non-legislative reforms are still to be implemented to align with the international framework on the processing of personal data and privacy.**

90. **While the efforts of Australia to update its privacy framework for personal data has been a prolonged process, if key recommendations from the Privacy Act Review process are prioritized and implemented, federal privacy law will be strengthened to align the right to privacy at the national level with the robust framework of privacy principles that exist at the international level. Furthermore, if the Government has the political will and resources, it could also focus on cross-jurisdictional harmonization of federal and state/territory-level privacy laws. and be an example for other federalist States.**

91. **The right to privacy is contained in the Universal Declaration of Human Rights and in the International Covenant on Civil and Political Rights, to which Australia is party. Introducing a federal human rights act would strengthen the country's link to the international legal framework.**

92. **It would be an important step for the Government to adopt a federal human rights act to increase awareness, strengthen protection measures and ensure that citizens can challenge alleged violations, including to the right to privacy, by taking remedial action through the Australian Human Rights Commission and, if necessary, the courts.**

[68] See https://www.d4d.net/state-of-open-data/chapters/issues/indigenous-data/v2.

[69] See https://ovic.vic.gov.au/privacy/resources-for-organisations/understanding-culturally-diverse-privacy-aboriginal-and-torres-strait-islander-peoples-perspectives.

[70] See https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/7-privacy-beyond-the-individual/privacy-protocols-for-indigenous-groups.

[71] See https://cdn.prod.website-files.com/5af4dc294c01df9fc297c900/65a5a8b8023cc22dc9135583_IDCARE%20submission%20-Law%20enforcement%20capabilities%20cybercrime%20-%2014Dec2023.pdf, p. 8.

93. **Further government collaboration with national institutions and partnerships with the private sector are crucial to respect, protect and enhance the right to privacy, identify best practices and find solutions in moving towards a global harmonization of privacy regulations.**

94. **It is key to understand the intersectionality of personal dignity with gender, ethnicity, age and disability, as vulnerable groups have a heightened risk of privacy violations, online and offline, which can reveal alarming trends of discrimination, violence, sexual exploitation, cyberbullying and financial manipulation.**

A. Personal data protection

95. **The Special Rapporteur urges the Government to expedite the implementation of the remaining recommendations in the Privacy Act review to update, strengthen and better align federal privacy law with other international frameworks, based on the experience of other regions (Europe and the General Data Protection Regulation and the Ibero-American system and its associated standards and guidelines). Furthermore, a more harmonized legal framework at the state level is also encouraged as it remains fragmented**

96. **Data are very important assets, and citizens need confidence and trust in their data. The protection of personal data is a shared responsibility that must be balanced with the right to access and disclose, because if data are overprotected that could inadvertently result in enabling corruption. Thus transparency, privacy by design (minimalization of data collection and retention), privacy impact statements and regional and international standards for data protection mechanisms are essential tools.**

97. **The Special Rapporteur welcomes the establishment of a statutory tort for serious invasions of privacy. A key complementary element to improve access to redress would be to substantively increase the funding of the Privacy Commissioner to implement a more robust and effective complaints processing mechanism for breaches of privacy at the administrative level to minimize delays and reduce any backlog of complaints.**

98. **The Special Rapporteur urges the promotion of the use of e-systems, while recognizing the consequences of privacy versus convenience, and the role of the eSafety Commissioner, who is responsible for online safety and provides guidance to various communities who are at greater risk of online harms, including specialized support in relation to gender, sexuality and race. The eSafety Commissioner requires additional resources and support to effectively carry out its mandate.**

99. **The Special Rapporteur encourages the Government and the private sector to increase cooperation and standardization through a joint programme to more widely apply and reinforce the Guiding Principles on Business and Human Rights.**

B. Privacy and health data

100. **The COVID-19 pandemic highlighted the positive and negative impacts of the increasing use of applications and digital solutions in patient healthcare. The Special Rapporteur encouraged the Government to further reflect on the recommendations on implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of a pandemic.**[72]

101. **The Special Rapporteur welcomes the Government's transition to an e-system but stressed the importance of robust security measures to ensure secure collaboration among healthcare providers managing sensitive health data. E-health records and the use of artificial intelligence and technology require stringent measures and patients'**

[72] A/HRC/52/37, paras. 27–32.

data need standardization and harmonization to adhere to the highest standards of privacy.

102. **As medical services are administered at the state level, the Department of Health and Aged Care must: ensure that health professionals and personnel respect patients' right to privacy and dignity by taking measures to guarantee that all systems, procedures, records and data collection securely protect the confidentiality of all medical or other treatments; and ensure that policies and regulations are consistent across the country.**

C. Emerging technologies

103. **Technological innovation in artificial intelligence, biometrics, facial recognition technology and neurotechnology must be implemented using a human rights-based approach to mitigate the risks of inadvertent misuse and intentional abuse that can result in serious privacy infringements.**

104. **Government and business have a joint responsibility to cooperate with academics, civil society and technology companies to ensure a holistic approach so that citizens understand the consequences and importance of responsible use of emerging technologies, such as artificial intelligence**[73] **and neurotechnology,**[74] **to effectively protect the right to privacy.**

105. **To ensure that the legal framework remains resilient, policies and regulations must be sufficiently flexible to align with rapidly advancing technological developments and contain robust legal safeguards that are harmonized with international norms.**[75] **That will ensure a more effective complaints system and that remedies are accessible, in practice, to effectively address data breaches and privacy violations, particularly in an increasingly digital age that requires flexible and innovative technical solutions towards social progress that do not undermine the right to privacy.**

106. **The Special Rapporteur encourages the Government to take up a leadership role in promoting international cooperation to implement the General Assembly resolution on seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development.**[76]

D. Cybersecurity and cybercrime

107. **The Special Rapporteur welcomes the implementation of the Cyber Security Act with enhanced safeguards and increased accountability, which are key in ensuring a coordinated approach to cybersecurity threats affecting the personal data of individuals.**

E. Surveillance and oversight

108. **The public's trust in the operation of the law enforcement and intelligence communities is essential as the operations carried out by the relevant agencies are necessarily exercised in a covert manner. The Special Rapporteur acknowledges the ongoing efforts made by Australia to strengthen the legal framework and urges the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security to continue to apply their oversight powers to surveillance and interception of telecommunications to ensure necessity and proportionality in the investigation of crimes and security threats, while protecting the right to privacy of legitimate users of online platforms.**

[73] See A/78/310.
[74] See A/HRC/58/58.
[75] See A/HRC/55/46.
[76] General Assembly resolution 78/265.

109. **The Special Rapporteur recommends that law enforcement personnel, prosecutors and judges receive adequate training to enable them to conduct privacy impact assessments and evaluate the quality of the data so that they better understand the possible consequences of the use of the emerging technologies they are regulating.**

110. **The Special Rapporteur recommends that the Government strengthen the capacity of all security systems, networks and data technology so they are upgraded in accordance with the regulations of the International Criminal Police Organization so that when Australia shares personal information or intelligence with other countries its systems reinforce adequate privacy safeguards for cross-border intelligence sharing.**

111. **Facial recognition technology is becoming widespread in Australia. The Special Rapporteur strongly recommends that more education is provided on the use of facial recognition technology and the impact of the right to privacy.**

112. **While decisions of the Australia Human Rights Commission are non-binding, the Commission can play a pivotal role in raising greater awareness of the various types and levels of privacy infringements and violations by robustly monitoring such infringements and violations and ensuring that the judiciary and administrative bodies respect their legal obligation to impose sanctions and provide effective remedies in an era of increasing digital surveillance. Therefore, it is essential that the Commission is adequately financed so its recommendations can be implemented in national laws, policies and programmes.**

F. Gender

113. **Australia has ratified the International Covenant on Civil and Political Rights and the Special Rapporteur encourages the Government to recognize that the right to privacy includes the right to self-determination on gender and the freedom of individuals to make autonomous decisions about their bodies.**

114. **The Special Rapporteur reminds the Government of the Human Rights Committee reiteration that the right to privacy covers gender identity.**[77] **Australia has a duty to uphold the right to privacy in relation to gender identity**[78] **and recommends that the principles outlined by her predecessor regarding gender identity and legal recognition be respected and implemented.**[79]

115. **The Special Rapporteur calls upon the Government to be guided by the Yogyakarta Principles on the Application of International Human Rights Law in relation to Sexual Orientation and Gender Identity and their update, known as the Yogyakarta Principles plus 10, to ensure legal recognition of individuals' gender identity without imposing intrusive and onerous requirements.**

116. **The Special Rapporteur urges the Government to ensure that personal information relating to sex and gender is protected through regular vulnerability assessments of information management systems and regular training for staff on data privacy and data security.**

117. **The Special Rapporteur reminds the Government of the grounds on which special categories of data can be processed. One of them is the consent of the data subject, to protect personal health data related to reproductive health, sexual orientation and gender identity.**

G. Children

118. **Australia has made efforts to promote and protect children's privacy, in accordance with the rights and values of the Convention on the Rights of the Child, but**

[77] See CCPR/C/119/D/2172/2012.
[78] Human Rights Council resolution 34/7, para. 5 (g).
[79] A/HRC/43/52, paras. 35 and 36.

to further safeguard their autonomy, in both the digital and non-digital spheres, it is necessary to strengthen policies, laws and regulations to incorporate specific strategies that reflect child privacy impact assessments before introducing innovations, including those intended to reduce the risks of cyberbullying, online exploitation and abuse of children and young people, to avoid inadvertent and harmful impacts and ensure that children have effective remedies against privacy infringements.

119. **The Special Rapporteur notes the effective partnership of the United Nations Children's Fund in Australia with the Centre of Excellence for the Digital Child to improve the digital world for children and encourages implementation of the Manifesto for a Better Children's Internet.**[80]

120. **The Special Rapporteur recommends that the Government facilitate further involvement of civil society organizations working in the field of children's rights in the development, implementation, monitoring and evaluation of laws, policies and programmes to protect the dignity and privacy rights of children.**

121. **The Special Rapporteur reminds the Government of the invaluable guidance provided by the Committee on the Rights of the Child in its general comment No. 25 (2021) on children's rights in relation to the digital environment. In general comment No. 25 (2021), the Committee recommended that the business sector undertake child rights due diligence, and child rights impact assessments, as well as implement regulatory frameworks, industry codes and terms of services that adhered to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services.**

122. **The Special Rapporteur recommends that the Department of Education, in coordination with the Department of Health and Aged Care, educate teachers and provide specialized counsellors to inform children, from an early age, of the importance of understanding that they control their sphere of privacy, to mitigate the threat of online activities aimed at the sexual exploitation of youth.**

123. **In their implementation of the Convention on the Rights of the Child, which Australia ratified in 1990, the Committee on the Rights of the Child urged States to repeal all laws criminalizing or otherwise discriminating against individuals on the basis of their sexual orientation, gender identity or intersex status and to adopt laws prohibiting discrimination on those grounds.**[81]

124. **The Special Rapporteur encourages the Government to take into consideration her predecessor's recommendations on children and privacy**[82] **and prioritize digital education for children, in age-appropriate language, on exercising their rights to privacy and ensure that there are provisions for counselling and administrative and judicial complaint mechanisms.**

125. **Regarding the proposed minimum age (16 years) for social media use, the Special Rapporteur urges the Government to consult further with the eSafety Commissioner and civil society who advocate for children's rights to find solutions to ensure that there is a balance between monitoring social media use and protecting the safety and mental health of children. Furthermore, it is important to seek assurances that privacy rights will be adequately protected as the introduction of those measures may require providing biometrics or identity information.**

H. Vulnerable groups

126. **The Australian Human Rights Commission investigates and resolves complaints regarding violations but the Special Rapporteur noted a lack of trust and accessibility to national institutions among some sectors of society (such as Indigenous persons and**

[80] See https://issuu.com/digitalchild/docs/childrensinternet_interactive-1.
[81] Committee on the Rights of the Child, general comment No. 20 (2016), para. 34.
[82] A/HRC/46/37, para. 127.

LGBTQI+ persons), which can result in a reluctance to bring forward a complaint at either the administrative or judicial level.

127. **Encourage the Government to take a greater role on the international stage in relation to digital rights and implement strategies to leave no one behind, as enshrined in the 2030 Agenda for Sustainable Development and its Sustainable Development Goals, in an increasingly digital age, especially regarding vulnerable groups such as the elderly, Indigenous populations and those in rural communities.**

128. **It is critical to build trust and elevate digital literacy among marginalized groups by organizing workshops to enhance understanding of safety and privacy when accessing various online services, to close the digital divide since increased reliance on emerging technologies will continue to evolve.**