March 31, 2023

To:

The Attorney-General's Department,
Australia
Email: PrivacyActReview@ag.gov.au

Submission to the Australian Attorney-General's Department on the Review of the Privacy Act 1988 - comments on the 2022 Report

We thank the Attorney-General's Department for the opportunity to submit comments on the 2022 Report published as part of the advancing process in the Review of the Privacy Act 1988.

About Access Now

Access Now is an international non-profit organization which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations.[1]

Access Now actively engages with authorities across the world, including in Australia, on protecting human rights in the digital age. We had submitted joint comments to the Attorney-General on the Issues Paper as part of the review of the Privacy Act 1988, and provided detailed individual comments in January 2022 to the consultation organized by the department .[2] We had also made a submission to the Department of Infrastructure, Transport, Regional Development and Communications on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021; and to the Cyber Security Policy

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, *Australia's privacy laws are getting an update — here's what we recommend*, https://www.accessnow.org/australias-privacy-laws-recommendations/

Division, Department of Home Affairs, on Australia's 2020 Cyber Security Strategy.[3] Access Now provided recommendations on the cyber security infrastructure in Australia through a report titled " Human Rights in the Digital Era: An International Perspective on Australia".[4] We participated in the public hearings, as well as made written submissions, on the implications of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 on human rights, and the changes that are necessary, to the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.[5]

At the outset, we are glad to see the continuing focus from the Attorney-General on reforming Australia's privacy legal framework to better protect human rights and to meet international best standards with respect to data protection. It is crucial that this focus remains undiluted and results in specific legislation brought to the Australian Parliament this year in order to comprehensively amend the Privacy Act 1988.

In our January 2022 submission, we had outlined eight priority areas where we believed key reforms had to be undertaken, building on our global recommendations for policymakers on data protections "do's and don'ts".[6] Our 2022 inputs focused on:

- Personal information, de-identification and sensitive information
- A statutory tort of privacy
- A direct right of action
- Consent to collection, use and disclosure of personal information; and Additional protections for collection, use and disclosure
- Pro-privacy default settings
- Security and destruction of personal information
- Restricted and Prohibited Practices
- Political exemption

[3] Access Now, *Submission on Australia's 2020 Cyber Security Strategy*, https://www.accessnow.org/cms/assets/uploads/2019/11/Consultation-Australia-2020-cybersecurity-strategy-1-November-2019-.pdf

[4] Access Now, *Human Rights in the Digital Era: An International Perspective on Australia*, https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf

[5] Access Now, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, https://www.inslm.gov.au/sites/default/files/2019-11/32._access_now.pdf

[6] Access Now, Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers, https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf, November 2019.

We are heartened to note that the December 2022 report published by the Attorney-General's Department builds on many of the positions we advanced in our recommendations, and contained specific legislative proposals for consideration. We provide our initial inputs to priority areas we identified in the 2022 Report and provide recommendations for enactment or reconsideration of several of the specific proposals there. These are currently our initial recommendations and are not exhaustive; we believe that the Attorney-General's Department should further consult with stakeholders, particularly public interest technologists and civil society, over the next few months as it finalizes its final set of legislative proposals to bring to Parliament later this year.

Summary of initial inputs on proposals in 2022 Report in Privacy Act review

Subject area proposed in Privacy Act Review 2022 Report:	**Our recommendation regarding key specific proposals in this area:**	**Our additional detailed comments on the issue, if any:**
Objects of the Act	We recommend enactment of Proposal 3.2:	We agree with the intention to clarify the wider public interest in protecting privacy and that recognising this will help inform balancing exercises when they are conducted. Protecting privacy has both individual interest and wider public interest. This recognition is also crucial in its implication that the right to privacy ought not to be restricted based on overbroad and vague "public interest" justifications.
Personal information, de-identification and sensitive information	We recommend enactment of proposals 4.1, 4.2, 4.3, 4.4, 4.5, 4.9, 4.10 We recommend further consultation of proposals 4.6, 4.7, and 4.8.	Any definition of personal information must include technical and inferred personal information, supported by a non-exhaustive list of the types of information capable of falling within the new definition, objective factors to assist entities to determine when an individual is reasonably identifiable, and a definition of "collection" that expressly covers "inferred" information. We believe that the term "about" in the definition of personal information should be replaced with "relates to". We recommend that the proposal amend the

		law to clarify that “inferred” information includes “generated” information. This would ensure that new information generated about an individual – such as customer ratings, predictions of individuals’ behavioral patterns, or buying preferences – is within the ambit of the definition of personal information. We support calls to amend the Act to require information to be “irreversibly anonymised” rather than “de-identified” for the Act to no longer apply. The higher threshold of anonymity, which can be met only once it is no longer possible to identify an individual from the information, will be far more effective in practice for meaningfully protecting privacy. Fully anonymised data is not easily achievable and in practice, it is difficult to claim that data is in fact fully anonymous as it can often be attributed back to an individual. Therefore, this higher threshold is necessary. We also support calls to clarify that genomic information is sensitive information, and that sensitive information can be inferred from information that is not sensitive.
Flexibility of the APPs	We recommend enactment of proposals 5.1, 5.2.	We believe that it is important to provide a regulatory backstop in case co-regulatory approaches may not actually be advanced sufficiently by industry actors on their own initiative.
Political exemption	We recommend enactment of proposals 8.1, 8.2, 8.3, 8.4, 8.5, and 8.6.	The Privacy Act should protect people's privacy in the digital age in a holistic manner, without vast exemptions, particularly for entities that play a crucial role in the democratic processes of the country and therefore owe accountability to the people. As an ancillary benefit, elimination of the exemption would also contribute towards

		restoring the integrity of and public trust in the electoral process. Such elimination is vital not only to protect people's privacy but also to safeguard democracy itself.
Privacy policies and collection notices	We recommend enactment of proposals 10.1, 10.2, and 10.3.	At present, privacy policies and collection notices are often voluminous and incomprehensible to the average individual, rendering them meaningless. They must be devised in a clear, comprehensive, concise, and easily understandable format, in order for them to be meaningful sources of information to individuals, empowering them to make informed decisions regarding their data.
Consent and privacy default settings	We recommend enactment of proposals 11.1, 11.2, 11.3, and 11.4	We support the approach of requiring that consent be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action. This would mean, in practice, that this consent model would be on the basis of informed, up-to-date and specific opt-in requirements, as opposed to an opt-out system with options pre-selected for a user, which could not be considered "voluntary" or "unambiguous". To strengthen the consent requirement, we recommend that the user also be given an explicit right to withdraw consent at any point in time.
Fair and reasonable personal information handling	We recommend enactment with modification of proposals 12.1 and 12.2. We recommend enactment of proposal 12.3 following further consultation with	With respect to additional protections for collection, use and disclosure, the proposal in the original Discussion Paper stated that the collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances, and lists factors relevant to this assessment. We recommend that to enable optimum protection of rights, collection, use or

	stakeholders.	disclosure of personal information must also be lawful, in addition to fair and reasonable. The lawfulness requirement is necessary to ensure that information is processed on a clear legal basis, for a lawful purpose. We note the reference to fair and reasonable is not consistent with the international standard (which namely focuses on "necessary and proportionate"), which most effectively aligns with the goal of protecting rights. However, it may be a first step for oversight over data handling. The principle should however be clearly defined and enforced by regulator, in a manner that's harmonious with necessity and promotional standards, to ensure that people's rights are at the center of the application of this concept" We therefore recommend that the standard adopted should include a requirement for "lawful" in addition to "fair and reasonable", if the standard of "necessary and proportionate" is not adopted wholesale.
Additional protections	We recommend enactment of proposals 13.1, 13.2, 13.3, and 13.4 following further consultation with stakeholders.	We welcome the recognition of increased regulatory requirements and data protection measures for areas that have significantly increased intrusion on privacy, including facial recognition technology. We believe however that this required further consultation with stakeholders in order to determine if even stronger measures should be advocated for.
Rights of the Individual	We recommend enactment of proposals 18.1, 18.2, 18.3, and 18.4., following further consultation with stakeholders to ensure the most strengthened text of these rights are	Protecting users' data protection and guaranteeing their control over their personal information requires establishing a series of binding rights to exercise, including: Right to access ; Right to object; Right to erasure; Right to rectification; Right to information; Right to explanation; and the Right to portability. Although this list is not exhaustive, these rights

	advanced. We recommend that proposals 18.5 and 18.6 be advanced after further consultation with stakeholders.	must be provided for by law, and not left to the discretion of entities using the data. Users shall be able to exercise any of these rights free of charge. We advise careful discussions of the exact textual formulation of the right to de-indexing and appreciate the careful enunciation of that proposed right by the Attorney-General's Department.
Automated decision making	We recommend enactment of proposals 19.1, 19.2, and 19.3,following further consultation with stakeholders.	In addition to ensuring transparency and accountability in respect of the use of automated decision-making tools, we recommend imposing limitations on their use in the context of certain types of sensitive personal information. The biases and errors of automated decision-making tools have been well-demonstrated. Their application to process personal data under certain circumstances, such as to glean the characteristics and traits of individuals to create, and potentially share, personal profiles, can be deeply problematic, and violative of people's rights and autonomy.
Security, retention and destruction	We recommend enactment of proposals 21.1, 21.2, 21.3. We recommend further consultation with stakeholders on whether and how to advance proposals 21.3 and 21.4. We recommend enactment of proposal 21.6 after further consultation with stakeholders.	We welcome the recognition of the shared interests in effective cybersecurity measures and data protection best practices. We also appreciate the recognition that data retention measures can have on data protection and undermine privacy standards as a whole. We advise that the further discussions around the data retention proposal would benefit from further discussion with stakeholders engaged in some of the existing review mechanisms that have been initiated in that area, and sharpen the focus for reforms in the Privacy Act and its horizontal application.

Overseas data flows	We recommend enactment of proposals 23.1, 23.2, 23.4, and 23.5. We recommend further consultation with stakeholders on whether and how to advance proposals 23.3 and 23.6	As we noted in our 2019 data protection global guidance for policymakers, in the digital age, it can be difficult for legislators to ensure sufficient protection of personal data and the rights of users without applying the principle of extraterritoriality. To understand the benefits of the extension of the jurisdictional scope of data protection, we need to look at the issue not from an "establishment" perspective (where is the entity located) but from a user's perspective (where is the user and where is the user from). The objective of human rights law, such as data protection frameworks, is first and foremost to protect individuals at all times. It is therefore logical to ensure that users' rights are respected no matter where the entities using people's data are located. Extending the scope of jurisdiction is not a one-size-fits-all solution and specific criteria should be established in data protection laws to limit bad copies or harmful consequences. Lawmakers should for instance clearly indicate under which scenarios the law applies outside their borders, to which actors specifically, what enforcement mechanisms will be in place, and provide users, companies, and authorities with clear avenues for remedies.
Enforcement	We recommend enactment of proposals 25.1, 25.2, 25.3, 25.4, 25.5. 25.9, and 25.10. We recommend further consultation with stakeholders on whether and how to advance proposals 25.6, 25.7, 25.8, and 25.11.	We support the provision of enhanced civil penalties and investigative, inquiry powers for the Information Commissioner. We welcome the efforts made to provide enhanced legal remedies for individuals via the courts, but recommend further discussion on whether the federal court and other named courts in the proposal are the best fora for such civil penalty provisions. We advise further discussion and consensus with public interest groups and independence voices on whether industry

		funding models are appropriate for the OAIC or whether increased public funding is a better option. We also advise further discussion around contingency litigation funding.
A direct right of action	We recommend enactment of proposals 26.1 after further consultation with stakeholders on the ideal design elements of this right.	We support the proposal to create a direct right of action. In addition to individuals or groups of individuals whose privacy has been interfered with, the action should also be available to non-governmental and non-profit organizations to represent users and to independently bring complaints and cases before the OAIC and courts. This will also help mitigate the issue of accessibility of the right of action owing to the expansive resources often necessary for litigation. In order to ensure that there are no delays and bottlenecks, the OAIC must be required to complete its assessment of the claimant's complaint within a specified time period. In the interest of transparency and accountability, the OAIC must be required to make its assessment of a complaint available in writing. This would also help better inform the court procedure that may follow. In addition to the OAIC, individuals as well as organizations with expertise in the field should be permitted to appear as amici curiae to provide expert evidence. The benefits of such expert evidence have been well documented through the judgements pertaining to the right to privacy by courts in various jurisdictions including the European Court of Human Rights and the Court of Justice of the European Union (CJEU).
A statutory tort for serious invasions of privacy	We recommend enactment of proposal 27.1	A statutory tort for invasion of privacy is a crucial element of an effective data protection regime that confers an enforceable right on individuals to seek redressal for violations of the right to privacy. Meaningful penalties and

		statutory damages stemming from the tort will also augment accountability from digital service providers and fuel privacy-centric innovation. A statutory cause of action is necessary given the increasing instances of invasions of privacy by intrusion and misuse of personal information, and to honor Australia's commitment to the International Covenant on Civil and Political Rights, which requires countries to protect the privacy of its citizens. Further, in order to implement a robust rights-based framework, in addition to the statutory tort, the government must incorporate a federal level right to privacy in line with Article 12 of the United Nations (UN) Universal Declaration of Human Rights to which the Australian government is a signatory. Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." A statutory tort provides an important avenue for remedy to the affected individuals and serves as an economic model that incentivises responsible data practices on the part of companies. However, recognising the right to privacy at a federal level will go a step further. It will propel long-term change in policy and innovation in that data will be governed through a rights-based approach as opposed to a merely value-driven one.
Notifiable data breaches scheme	We recommend enactment of proposals 28.1 and 28.2 after further consultation with stakeholders.	We welcome the improvements being made on data breach notification. We recommend that efforts be made to allow for better coordination across Australian agencies on the issue of data breach, including movement to a single window mechanism for data breach

		notification to the Australian government in addition to notification to impacted individuals.
Interactions with other schemes	We recommend enactment of proposals 29.1, 29.2 and 28.3 after further consultation with stakeholders.	We welcome the proposals made to improve cross-agency coordination and capacity building on privacy obligations, and improved regulatory cooperation. We believe that part of this would also be impacted by outputs of the electronic surveillance review and urge a holistic approach to inter-department and commonwealth-state cooperation.

Conclusion

Thank you for the opportunity to participate in the latest round of consultation in the Privacy Act Review, which we hope will result in legislative proposals brought to the Australian Parliament this year. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org

Access Now | https://www.accessnow.org

[*This submission was prepared with the benefit of our global data protection policy recommendations maintained by Estelle Massé, Global Data Protection Lead at Access Now*]