January 10, 2022

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

We thank the Attorney-General's Department for the opportunity to submit comments on the Review of the Privacy Act 1988.

About Access Now

Access Now is an international non-profit organisation 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. 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 Division, Department of Home Affairs, on Australia's 2020 Cyber Security Strategy.[2] Access Now provided recommendations on the cyber security infrastructure in Australia through a report titled "

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] 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

Human Rights in the Digital Era: An International Perspective on Australia".[3] 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.[4] Further, we are concerned by the consistent development of an apparatus of surveillance laws in Australia, including through the recently passed Surveillance Legislation Amendment (Identify and Disrupt) Act 2021.[5]

We write to you to provide our comments based on our expertise working on digital rights in Australia, and various regions across the world.

Comments on the Review of the Privacy Act 1988

The review of the Privacy Act 1988 ("Act") is an important step towards ensuring that Australians' right to privacy is protected, and people's autonomy over their information is prioritised in the digital age. The multiplicity and ubiquity of digital services and internet intermediaries, and unchecked practices of data collection, usage and sharing, combined with lack of transparency and effective legal safeguards to protect people's rights, have made it imperative for the Act to be amended. We support many of the proposals put forward in the Privacy Act Review discussion paper[6], and provide comments for improvement of certain proposals.

Personal information, de-identification and sensitive information

We endorse the proposed definition of personal information to 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 also welcome the proposal to replace "about" in the definition of personal information with "relates to".

We recommend that it be clarified that "inferred" information includes "generated" information. This

[3] 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
[4] 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

[5] Access Now, *Surveillance state incoming with Australia's "hacking" bill*, https://www.accessnow.org/surveillance-state-incoming-with-australias-hacking-bill/; Access Now, *To protect human rights, identify and disrupt Australia's "hacking bill"*, https://www.accessnow.org/to-protect-human-rights-identify-and-disrupt-australias-hacking-bill/
[6] Attorney General's Department, Australian Government, Privacy Act Review Discussion Paper, October 2021.

would ensure that new information generated about an individual – such as customer ratings, predictions of individuals' behavioural patterns, or buying preferences – is within the ambit of the definition of personal information.

Further, we support the proposal to amend the Act to require information to be "anonymous" 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.

Question in the Discussion Paper: In practice, what types of information would the proposed definition of personal information capture which are not presently covered?

Below is a non-exhaustive list of the types of information that the proposed definition in the Discussion Paper would cover:

- IP addresses and other device identifiers;
- Metadata and location data;
- Cookies, web beacons, trackers, and similar digital identifiers;
- Behavioural patterns discerned from wearable devices or analysis of online activities;
- Purchasing preferences of customers;
- Data garnered from smart devices including cars, televisions, fitness trackers, home devices, etc.;
- Predictions and extrapolations about a person's likes, preferences, and patterns whether they are accurate or not;

A statutory tort of privacy

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.

We support Option 1 in the Discussion Paper to introduce a statutory tort for invasion of privacy as recommended by the Australian Law Reform Commission Report 123. As recommended by the ALRC in 2014[7], a statutory tort for invasion of privacy should be enacted to address the deficiencies in the existing regime. A statutory cause of action is necessary given the increasing instances of invasions of privacy by intrusion and misuse of personal information, and to honour Australia's commitment to the

[7] Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (ALRC Report 123), September 2014.

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 honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[8] 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.

A direct right of action

Question in the Discussion Paper: Is each element of the proposed model fit for purpose? In particular, does the proposed gateway to actions strike the right balance between protecting the court's resources and providing individuals a more direct avenue for seeking judicial consideration and compensation?

We support the proposal to create a direct right of action. We make the following summary recommendations to inform and amend the evolving design elements of this right as laid down in the Discussion Paper:

- 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 organisations to represent users and to independently bring complaints and cases before the OAIC and courts.[9] 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 organisations with expertise in the field should

[8] United Nations, Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights
[9] 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.

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).

Consent to collection, use and disclosure of personal information; and Additional protections for collection, use and disclosure

We endorse the proposal 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.

Question in the Discussion Paper: Should entities be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information?

Yes. The Discussion Paper, in its definition of consent, already suggests that consent must be obtained afresh when the purpose for the collection, use or disclosure of personal information changes. However, in any addition to when the purpose changes, where sensitive information is involved, consent must also be renewed when there is a change in the method of storage or retention of data; in the nature or number of third parties with whom data may be shared, or individuals or entities that may have access to the data; in the overall policy of the service provider impacting data collection, use and disclosure. This is in fact necessary to ensure that consent is "specific" as it is so in relation to specific purposes and processing activities; any changes in these operations implies a need to obtain consent. This is a non-exhaustive list and any material change in the conditions under which consent was first obtained should result in a request for renewal of consent to ensure that users are empowered in a continuing manner to exercise autonomy and make an informed decision on the treatment of their personal information.

With respect to additional protections for collection, use and disclosure, the proposal in the Discussion Paper states 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 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.

Pro-privacy default settings

Question in the Discussion Paper: Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?
We support Option 1 – Pro-privacy settings enabled by default: "Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation."

Option 1 would enable users to have their privacy right protected by default and make an active expression of individual choice. It is therefore aligned with the fifth element of consent set out in the Discussion Paper, i.e., unambiguous indication through clear action. As Recital 32 of the GDPR states, "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent".[10] As the Discussion Paper rightly recognises through an example, "[t]he pre-checked consent box is also unlikely to constitute an unambiguous indication of the individual's choice through clear action."

Further, pro-privacy default settings embody the principle of data protection by design and default, which bolsters data security and integrity. When entities embed privacy-centric design by default in their product and service development at the very outset, they save costs later in the process as fewer adjustments would be necessary for compliance. Such an approach also enables the creation of a culture of accountability in data protection, as opposed to it being perceived as a tedious compliance requirement.

Question in the Discussion Paper: If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?

The following is a non-exhaustive list of types of personal information handling practices should be disabled by default:

- Handling for any purpose other than those for which voluntary, informed, current and specific consent has been obtained through an unambiguous indication through clear action;
- Handling that is not necessary to enable the provision of the specific product or service;
- Handling that entails disclosure to third parties that is not necessary for the provision of the specific product or service;
- Retention of data for an indefinite or unreasonable period of time that extends beyond the period necessary for provision of the product or service;
- Profiling, tracking or monitoring the behaviour of the user, those they interact with, or look-a-like audience,
- Registration or subscription to services, newsletters, or platforms without the explicit request and consent of the user;

[10] EU GDPR, Recital 32, https://www.privacy-regulation.eu/en/recital-32-GDPR.htm.

Security and destruction of personal information

Robust cyber security infrastructure is crucial to the implementation of a privacy and data protection regime. A key element of strong cyber security that protects individual privacy, the economy as well is national security, is encryption.[11] Attacks are mounting against encryption in Australia, including through the Telecommunications and Other Legislation Amendment (Assistance and Access) Act, the Identify and Disrupt Act, and the Draft Online Safety (Basic Online Safety Expectations) Determination. In order to meaningfully protect privacy, amendments to the Privacy Act must proactively protect and strengthen encryption, and other digital security tools that safeguard privacy.

The review of the Privacy Act presents an opportunity for Australia to act as a global leader in decisively prohibiting measures that undermine encryption, or force developers to modify their products to ensure exceptional or backdoor access by law enforcement or intelligence, and we strongly recommend that this opportunity be taken in the interest of human rights. Further, entities must have an obligation to resist orders that undermine security measures, including strong encryption, on grounds that are not necessary or proportionate.

Question in the Discussion Paper: What is the best approach to providing greater clarity about security requirements for APP entities?

Further, the proposal in the Discussion Paper suggests amending APP 11.1 to state that 'reasonable steps', to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure, includes technical and organisational measures; and to include a list of factors that indicate what reasonable steps may be required. We support this proposal.

We appreciate that APP 11.1 is expressed in a technology neutral manner in order to enable flexibility for APP entities to employ reasonable measures, as necessary, to protect personal information. Technology neutral language also helps prevent a situation where policies fail to keep pace with technological innovation and prescribe security measures inferior to those that may develop with time. However, a certain baseline standard of necessary security measures must be established, even if it is through negative obligations.

To this end, building on the recommendations in our "Human Rights in the Digital Era: An International

[11] Access Now, Policy Brief: 10 Facts to Counter Encryption Myths, https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf, 2021.

Perspective on Australia" report[12], and our submission on Australia's 2020 Cyber Security Strategy[13], we make the following summary recommendations with respect to the list of factors meant to indicate what may constitute "reasonable steps" :

- Consider the sensitivity of the personal information held;
- Resist efforts, policies and measures that undermine digital security measures, including strong encryption, on grounds that are not necessary or proportionate;
- Establish a vulnerabilities disclosure process and protect security research;
- Invest in research and development of strong digital security tools to protect Australians' data and rights;
- Employ a privacy and security by design approach that incorporates privacy and security as the central tenets at all the stages of data collection and processing;
- Commit to building cyber security policies and practices centered on human rights, including the right to privacy. Such policies and practices should include minimum cyber security standards which are a combination of specific and principles-based requirements;
- Strengthen data breach notification;
- Consider the impact of the security measure on the rights of individuals and the consequences of a breach for an individual. Create mandatory notification schemes which should ensure that the users are supported in how to protect accounts or information that may have been breached;

Restricted and Prohibited Practices

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

We emphasise that data protection frameworks must adopt a rights-based approach as opposed to a risk-based one.[14] Individuals must be empowered with the rights necessary to manage their privacy and exercise control over the handling of their personal information. The treatment of such information, and the fate of people's rights, should not be made contingent on a risk assessment conducted by the data processing entities.

---

[12] 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

[13] 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

[14] Access Now, The EU should regulate AI on the basis of rights, not risks, https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

As the Working Party 29 (an EU-level advisory body made up of representatives from national data protection authorities and the European Data Protection Supervisor) noted in a statement on the risk-based approach to explain that it cannot replace company obligations to protect our rights: ""…the Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance. The purpose of this statement is to set the record straight."[15] The statement further clarifies that "rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved".

A critical disadvantage of the risk-based approach outlined in Option 1 in the Discussion Paper is that risks are defined and assessed by entities that have an incentive to lower risk in order to be able to use the data. Therefore, the protection is not guaranteed or verifiable. The implementation of a clear framework on when and how data can be processed, backed by actionable rights, is much clearer for people and also gives legal certainty for entities processing data. If they have to assess risks and do it too loosely, they could be exposed to liability. Therefore, it is also in their interest to have a clear set of rules pertaining to the permissibility of certain data collection, use and disclosure practices, instead of matters being taken up for risk-assessment on a case-to-case basis.

Political exemption

People deserve a law that protects their 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.

There has been a massive uptick over the last decade in the practice of profiling and targeting individuals by political parties. Information privacy in the process of political campaigning needs to be addressed. The pervasiveness of personalised news feeds, political advertisements and other individual-targeted content online has made this exemption obsolete and detrimental to people's rights.

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.

[15] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

Conclusion

Thank you for the opportunity to participate in this consultation. 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,

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org

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

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

[*This submission was prepared with the assistance of Estelle Massé, Global Data Protection Lead at Access Now*]