

## **Joint comments to the Attorney-General on the review of the *Privacy Act 1988***

We, the undersigned organizations, would like to thank the Attorney-General for the opportunity to submit comments to the review of the Privacy Act 1988.

There is a growing need for this review as Australia continues to fall behind internationally in its understanding and implementation of privacy rights and protection of personal information. As the Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry final report indicated, there is an immediate need to reform Australia's approach to privacy and data protection in order to protect consumers in the digital era.<sup>1</sup>

**Updating the Privacy Act can give Australians the ability to control how their information is used and shared, and empower them to take action when their privacy is violated** at a time when the unchecked predatory data collection and aggregation of many digital services, advertisers, and Internet platforms is growing.

Prior to reviewing the Privacy Act's protections, we urge the government to enshrine in law 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."<sup>2</sup>

We believe that recognizing the right to privacy at the federal level is critical, in part as it will create a rights-based relationship with the way Australians' data is treated online, as opposed to an economic or value-driven model which has been the case so far. While a statutory tort may also be considered, it is only a partial substitute for implementing the right to privacy outright at the federal level.

Based on the issues paper presented by the government in October 2020 as a part of this review, our recommendations are as follows:<sup>3</sup>

1. **Redefine the scope and reach of the Privacy Act.** The Privacy Act must apply to any and all – public and private – entities which collect, process or otherwise handle personal data.
  - a. Privacy by design has been recognized as the international gold standard for new and emerging technologies while providing a great level of protection and certainty to individuals. This can help drive innovation in new services and products with privacy embedded in their developments.
2. **Apply strong safeguards to all types of personal information.** While the definition of personal information under the Privacy Act is good, we would urge the government to reconsider differentiation in the level of protection between this category and the special category of "sensitive information" which receives a higher level of protection.<sup>4</sup> Given the

---

<sup>1</sup> The ACCC Digital platforms final report provides several recommendations on how to strengthen the rights of consumers in the digital space, including stronger privacy protections and data rights:

<https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>

<sup>2</sup> [Universal Declaration of Human Rights | United Nations](#)

<sup>3</sup> [Privacy Act Review – Issues Paper – October 2020 \(ag.gov.au\)](#)

<sup>4</sup> [What is personal information? — OAIC](#)

ubiquity of technology and the way all our personal information interacts online and further information is inferred and generated continuously, this distinction seems arbitrary and all types of “personal information” deserve the same (highest) level of protection as afforded to sensitive information.<sup>5</sup>

- a. The discussion paper correctly identifies the need to address ‘technical data’ as metadata can often be equally as personal as other protected personal information. Technical data should therefore be considered in the definition of personal information and should enjoy the same level of protection.
3. **Adopt a rights-based approach.** In a data-driven economy, the rights of individuals should be the foundation of this review, and ensuring that Australians have direct rights of action when their privacy is violated or their personal information mistreated is essential in holding internet platforms, advertisers and malicious parties to account.
    - a. We urge the Attorney-General to consider the data rights granted under the EU General Data Protection Regulation (GDPR) and matched by many national data protection laws as a starting point for developing a similar rights-based system for the Australian context. While some rights, such as “the right to portability” already exist in Australia in specific circumstances, there are other vital rights under the GDPR such as the “right to explanation”, “right to rectification” and “right to erasure.”<sup>6</sup>
    - b. Specifically, the “right to explanation” is critical in helping individuals understand how their personal information was used in making decisions, creating accountability between individuals and the entity processing their information. This matter has been considered by the Australian Human Rights Commission in their discussion paper on Human Rights and Technology.<sup>7</sup>
  4. **Introduce a statutory tort for invasions of privacy.** One of the key components of a functional privacy or data protection regime is the ability for individuals’ rights to be enforced and for individuals to seek remedy. Establishing a statutory tort for invasions of privacy would greatly extend individuals’ ability to exercise their rights and keep entities processing their data (public or private) accountable.
    - a. The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such an avenue has increased as data harvesting practices are skyrocketing in Australia.<sup>8</sup> It was further suggested in the final report of the ACCC’s Digital Platforms Inquiry.
  5. **Consent should be introduced with a narrow definition.** We recognize that in the current digital ecosystem, consent is not always an effective way for individuals to control personal information, and can lose meaning. Consent should be required when information is collected and may be retained as long as data is used for the specified purpose of its collection. Consent should not be used as a way for individuals to sign any and all control and rights away as is

---

<sup>5</sup> The European Union’s (EU) General Data Protection Regulation (GDPR) has a much broader definition of personal data, which ensures a great level of protection for consumers and very little leeway for loopholes. Under the GDPR: “‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” [Art. 4 GDPR - Definitions - GDPR.eu](#)

<sup>6</sup> We recognize that the “right to erasure” has been misinterpreted globally and applied in very different ways across the EU member states. We would encourage the AG to consider the best practices for the Australian context. More in Access Now’s paper on the Rights to be Forgotten globally: [RTBF\\_Sep\\_2016.pdf](#) ([accessnow.org](#))

<sup>7</sup> [Human Rights and Technology | Australian Human Rights Commission](#)

<sup>8</sup> [Should a new tort be enacted? | ALRC](#)

often the case; the onus should remain on the organisations handling personal information to do no harm and collect, process, and store personal information in accordance with the appropriate legislation.

- a. Research conducted by The Australia Institute’s Centre for Responsible Technology highlights how the current consent and terms agreements on everyday sites are impregnable and legalistic, regularly allowing for changes without notice and held indefinitely.<sup>9</sup> Much clearer guard rails and red lines are required, even when consent is given by a user.
  - b. Ensuring the appropriate safeguards around consent for vulnerable populations (specifically children) also pose numerous challenges. Additional commitments such as legibility, a rights-based approach and specific design expectations similar to the UK’s Age Appropriate Design Code must be enshrined.<sup>10</sup> For more information please refer to Reset Australia’s individual submission.<sup>11</sup>
6. **Abolish exemptions, specifically the exemption for political parties.** Since exemptions from the Privacy Act were crafted over twenty years ago, they must be reconsidered. As we have seen through reports and documentaries such as *The Great Hack*, the exemption for political messaging poses a unique threat to our democracies.<sup>12</sup> Over the last decade we have seen an explosion in the practice of profiling and targeting individuals by political parties. Personalised news feeds, ads and other individual-targeted content online can more easily facilitate misinformation than offline political advertising could achieve. As a result, the risks posed – not only to the privacy of individuals but to the public good, including the stability of our democratic government and public trust in public institutions – have exponentially increased since 2000.<sup>13</sup>
7. **Individuals should have a right of action under the new rules.** The Office of the Australian Information Commissioner (OAIC) should have the powers and resources to launch independent investigations into organisations and to hear cases brought to them by individuals or representative NfPs. In that sense, they should be empowered to act as a guardian for individuals’ rights.<sup>14</sup>

Signed,

Access Now  
Centre for Responsible Technology Australia  
Digital Rights Watch  
Electronic Frontiers Australia  
Fastmail  
Reset Australia

---

<sup>9</sup> [Centre for Responsible Technology](#)

<sup>10</sup> UK Information Commissioner’s Office (2020) Age Appropriate Design Code. [Found online here.](#)

<sup>11</sup> <https://au.reset.tech/news/submission-on-the-review-of-the-privacy-act-1988/>

<sup>12</sup> [The Great Hack: the film that goes behind the scenes of the Facebook data scandal | Cambridge Analytica | The Guardian](#)

<sup>13</sup> For more about privacy as a public good see more from Salinger Privacy: <https://www.salingerprivacy.com.au/2020/08/10/privacy-is-a-public-good/>

<sup>14</sup> [Data-Protection-Guide-for-Lawmakers-Access-Now.pdf](#)