



**Australian  
Privacy  
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/About/Contacts.html>

9 April 2023

Privacy Act Review  
Attorney-Generals Department  
By email: PrivacyActReview@ag.gov.au

### **Privacy Act Review**

This submission is from the Australian Privacy Foundation (APF), the nation's pre-eminent and independent civil society organisation concerned with privacy. Information about the Foundation is available at [privacy.org.au](http://privacy.org.au). The submission builds on previous submissions in the Privacy Act review process, and previous reviews by ALRC touching on certain issues. Thanks for an extension to the submission date, and please accept our apologies for the delay.

Rather than repeat in detail the comprehensive points made in earlier APF submissions and in extensive efforts by other colleagues and privacy advocates, this submission identifies a short list of critical issues of agreement, and offers a few further observations.

Firstly we endorse the submission of APF board member and co-founder Prof Graham Greenleaf, available online on SSRN at <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4404413](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404413)> which reflects APF's current and historic concerns.

Secondly APF also supports recent submissions from consumer, human rights, research and NGO colleagues including experts such as Anna Johnston, Katharine Kemp, Vanessa Teague and Ed Santow, and organisations such as CHOICE (including their 'duty of care' model), Digital Rights Watch, EFA, CPRC and others. These are broadly consistent with our approach, and particularly useful on certain points. We would be happy to explain these on request.

### **Prof Greenleaf: "Focus on the key reforms - don't be distracted by the rest"**

Prof Greenleaf identifies a concern with the 116 recommendations in the most recent AGD consultation document, the *Privacy Act Review Report* of December 2022: the sheer number of proposals, and a lack of focus on which of them are most critical, as opposed to which are potentially useful but not necessarily essential. This is reminiscent of a similar problem with previous *Privacy Act* reform efforts, especially the exhaustive 2008 ALRC report (in the order of 3,000 pages) whose critical recommendations for a private right of action consistent with recommendations in previous ALRC reviews going back decades, and major reform in health records like EHRs, were among the many set aside.

We concur with Greenleaf's view of the key recommendations, which to enact or not, and the reasoning. See the summary table below, which we hope may simplify analysis and comparison of submissions. (The modification abbreviations are ours).

| Proposals   | Enact               | Enact with modifications   | Not Enact                       |
|---|---------------------|--|---------------------------------|
| 4.2–4.4 Expand definition of ‘personal information’, particularly so that ‘identifiability’ includes the capacity for ‘individuation’ or ‘interaction’ without requiring individual identification.   | 4.2,<br>4.3,<br>4.4 |  |                                 |
| 4.5–4.8 Avoid making ‘de-identified’ information a separate category mid-way between ‘personal information’ and anonymous information.  |                     | 4.5 + or capable of being distinguished from others  | 4.6,<br>4.7,<br>4.8             |
| 4.9–4.10 Expand ‘sensitive information’ definition  |                     | 4.9; 4.10 + genomic, inferred sensitive, geolocation tracking  |                                 |
| 6–9. Remove exemptions for small business, employee records, political and journalism as thoroughly and as swiftly as possible.   | 6, 7,<br>8, 9       |  |                                 |
| 11. Make definition of ‘consent’ more precise (and more like GDPR).   | 11.1,<br>11.3       | 11.4 default settings must be maximum protection.  |                                 |
| 12. Support proposal that processing in Australia ‘must be fair and reasonable in the circumstances’ (F&R) as foundation of the Act. But this must allow the whole purpose of a processing activity to be found to not be ‘fair and reasonable’ on an objective test. |                     | 12.1 if whole purpose not F&R, test fails.<br>12.2 factors to be in Act, not EM; additional factor.<br>12.3 F&R additional, not alternative to, consent. |                                 |
| 13. Go beyond Privacy Impact Assessments for high risk activities, by regulation which allows some to be prohibited, including by assessments that they are not ‘fair and reasonable’ activities.   | 13.1                | 13.1(b) any party can require PIA.<br>13.2, 13.3 more direct restrictions, & see 12.1–2.   |                                 |
| 15. Organisational Accountability - Purpose   |                     | 15.1 Secondary purpose F&R   |                                 |
| 18. Support the proposed new rights of the individual, but to also give individuals the right to require a determination by the OAIC on a dispute.  | 18.3–<br>5,<br>18.7 |  |                                 |
| 19. Strengthen rights re automated decision-making (ADM) by requiring notice at point of collection. Add right to ask questions, basis for complaint.   |                     | 19.3 notice of ADM and right to info at point of collection. Ask questions, refer to OAIC.   |                                 |
| 20. Support right to opt-out of direct marketing and targeting, if it is made stronger. Support requirement of consent for trading in personal information, but only if forced consent is prohibited.   |                     | 20.1 see modified 4.2.<br>20.2 1st part: add blanket opt-out.<br>20.3 F&R, & see 20.8(a). 20.4 trading not primary/secondary purpose.                    | 20.2<br>2 <sup>nd</sup><br>part |
| 22. Reject inclusion of a distinction between ‘controllers’ and ‘processors’.   |                     |  | 22.1                            |
| 25. Clarify enforcement powers. Reduce dismissal of complaints under s41 by giving complainants right to require s52 determination.   | 25.2;<br>25.4–<br>5 | 25.9 add complainant’ right to require determination.  |                                 |
| 26–27. Support both a direct right of action (with modifications), and the statutory tort.  | 27.1                | 26.1 no ‘gateway’ required; direct to FC/FCFCOA.   |                                 |

## Context

The relative consensus among stakeholders advocating for the interests of Australians whose personal information is at risk is consistent with growing community concern about the need for key changes in data protection and an effective, enforceable right to privacy.

### De-identification fails over time

We concur with Vanessa Teague’s observations about the failure of de-identification over time as a credible, reliable technical solution, given the risk of re-identification. Other research<sup>1</sup> and the increase in capabilities of machine learning and similar artificial intelligence (AI) tools to re-associate personal traits with ostensibly anonymised data, supports these concerns.

Greenleaf’s rejection of a hybrid category between ‘personal information’ and information which is truly anonymous is central to avoiding embedding this flawed method into the regulatory scheme, and reliance on de-identification should also be generally deprecated as reliable way to remove certain data from coverage of the Act.

### Data Minimisation – guiding principle for the future

In approaching this review, it is important to move beyond the commercial fascination with data maximalism – ‘data is the new oil’, ‘collect it all’, ‘lovely new data lakes, not boring old silos!’ – and efforts to shield its proponents from accountability for the consequences of their actions. Proponents had a good few years keeping growing calls for effective regulation at bay. But the recent proliferation of abuses, breaches and systemic threats arising from the avalanche of voracious new data-hungry AI tools appears to have finally triggered a correction in multiple jurisdictions. The best approach now is require plans to start from ‘data minimisation’, to avoid personal information becoming more of a ‘toxic asset’ as each new breach confirms it cannot really be protected. Requiring those who collect and deal with personal information to share the potential pain of the risk projected onto innocent victims, and to accept new expectations of transparency, foresight and a duty of care, should be the aim of revising the *Privacy Act*.

### Sectional interests

We caution against accepting special pleading from sectional interests, many of whom claim to be pursuing the public interest but are often primarily concerned with a conflicted private interest. In particular:

- Businesses who embraced the ‘data is the new oil’ rhetoric may prefer not to share the pain of the risks and breaches for which they are responsible as a result of data maximalism. Legitimising this preference is not a viable basis for corporate responsibility, or for incentivising others.
- The ‘Ad Tech’ industry: in recent years it had a chance to adopt privacy-respectful models but went all out on intrusive tracking, and now finds itself exposed as out of touch with popular

---

<sup>1</sup> See Marian-Andrei Rizoiu, Lexing Xie, Tiberio Caetano, Manuel Cebrian, ‘Evolution of Privacy Loss in Wikipedia,’ WSDM’16, Proceedings of the Ninth ACM International Conference on Web Search and Data Mining, 22–25 February 2016, San Francisco, pp 215-224, <<http://dx.doi.org/10.1145/2835776.2835798>>. Longitudinal erosion of the effectiveness of de-identification using AI/ML tools was not well understood. This example traced de-identified contributions over 13 years using features not apparently usable for re-identification, such as bare number of edits performed on very broad predefined categories in a given period. They show that even at such an unspecific level of behavioural profiling, it was possible to use off-the-shelf machine learning algorithms to uncover previously undisclosed personal traits, such as gender, religion or education, which contribute to risk of subsequent reidentification. They provide empirical evidence that the prediction accuracy for almost all private traits consistently improves over time, even for subjects who withdrew shortly after the start, as later insights from others can be applied retrospectively to a minimal profile. They proposed an open challenge: developing a physical model for ‘privacy loss’, i.e., predicting the de-anonymization rate of a given anonymized dataset over time; and suggest that this vulnerability would be characteristic of most de-identified data pools.

concerns triggered by its reliance on a ‘surveillance capitalism’ customer profiling model. Evolving AI capabilities to exploit such profiling for personalised manipulation feeds these concerns, as do questions raised about TikTok which in practice apply to the whole industry.

- Media industry submissions reportedly dismiss decades of good-faith efforts to carve out a wide domain for public interest reporting by in effect conflating ‘what the public might be enticed to click on’ with ‘what’s in the public interest’. Protection of individuals from unjustified intrusion is implicitly framed as only a private interest benefiting one (usually rich) person in the face of a broader public ‘right to know’ with no effective lower limits of triviality. Protecting privacy is however a competing public interest – one on which their own audience’s rights and freedoms may rely. APF has, with many other stakeholders, long supported special provisions for public interest journalism, including courts being required to balance privacy interests of any litigant against other important interests, especially ‘the public interest’ and in particular the needs of journalism.<sup>2</sup> So this apparent revival of exaggerated concerns about the practical impact of finally giving Australians the same entitlements to protect their interests as have long been enjoyed by citizens in almost all other developed countries is disappointing.

APF encourages bold and immediate legislative action to redress the lack of urgency sometimes seen in the past in respect of effective privacy protection, and to help Australians get ready to deal with the waves of new data threats on their horizon.

If you have any questions please do not hesitate to contact the author.

Yours sincerely

*(per)*

David Vaile

Chair

Australian Privacy Foundation

P: 0414 731 249

E: [chair@privacy.org.au](mailto:chair@privacy.org.au)

---

<sup>2</sup> See for instance the policies at <https://privacy.org.au/policies/right-of-action/> (2011) and <https://privacy.org.au/policies/media/> (2009), which include a long list of factors justifying collection or publication of personal information for the sort of public interest reasons used to justify investigative reporting, as well as other agencies’ and organisations’ activities. APF has also made submissions to the 2008 and 2014 ALRC Privacy Act reviews (and contributed to the reference panel in the latter) on similar lines, supporting a clear and usable public interest defence with media needs in mind. This includes support for the proposition that an injunction not be available unless a judge is satisfied that the justification for publication faces difficulties in being established, balanced against the degree of harm that the applicant's reputation or well-being would demonstrably suffer in the event of publication proceeding and being subsequently shown to be unjustified.