UNSW Law & Justice Research Series

Focus on the Key Reforms - Don't Be Distracted by the Rest

Graham Greenleaf

[2023] *UNSWLRS* 46
Submission to the Australian Federal Attorney-General on the *Privacy Act Review Report*

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Focus on the key reforms - don't be distracted by the rest (Submission to the Australian federal Attorney-General on the *Privacy Act Review Report*)

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney [**]

Background

In October 2021 the previous Australian federal government released two documents proposing reforms to the Privacy Act 1988: first, a draft 'Online Privacy Bill[1] including higher levels of regulation for online platforms, and more general strengthening of the Act's enforcement provisions; and second, a Discussion Paper (DP)[2] considering at least 70 options for a more extensive review of the Act, potentially the most extensive proposed changes to the *Privacy Act* since the inclusion of the private sector in its scope (2000).

By the change of government in May 2022, neither set of reforms had been enacted. However, over 200 submissions to the Attorney-General's Department (A-Gs) had been made, often critical of both the draft Bill[3] and of the Discussion Paper.[4] Post-election, A-Gs continued to consider the submissions received, and in December 2022 published the *Privacy Act Review Report*,[5] a 372 page report containing about 116 recommendations for reform under 30 main headings.

In response to the large scale data breaches by Optus and Medibank affecting millions of Australians, it became a political imperative for the Labor government to legislate a version of the previous 'Online Privacy Bill'. The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* passed both houses on 28 November 2022, and was assented to on 12 December 2022, commencing immediately. The Act included vastly increased maximum civil penalties, new regulatory powers for the Office of the Australian Information Commissioner (OAIC) and ACMA (Australian Communications and Media Authority), requirements to publish more details of Notifiable Data Breaches (NDB), and slightly stronger extra-territoriality provision (removal of the requirement for foreign entities to have an 'Australian link' to be liable, so now it is sufficient if they carry on a commercial activity in Australia). This Act does not include the previously proposed 'Online Privacy Code' imposing higher standards on platforms, or all of the proposed strengthening of enforcement. The

---

[**] The author's qualifications to make a submission are at the end of the submission.

[1] 'Online Privacy Bill Exposure Draft', including *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, and the Attorney-General's Department *Explanatory Paper*, October 2021 <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>.

[2] Australian Government *Privacy Act Review – Discussion Paper,* October 2021 <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>

[3] See for example Greenleaf, Graham and Kemp, Katharine 'Australia's Online Privacy Bill Targets Social Media Giants' (2021) 174 *Privacy Laws & Business International Report* 1, 5-9, < https://ssrn.com/abstract=4027702> , based on submissions on the draft Bill (hereinafter 'Greenleaf & Kemp Submissions on draft Bill')

[4] See for example in Greenleaf, Graham and Kemp, Katharine "Australia's Privacy Act Discussion Paper: 'All that Is Solid Melts into Air'" (2022) 175 *Privacy Laws & Business International Report* 22-26, <https://ssrn.com/abstract=4086263>, based on submissions on the Discussion Paper (hereinafter 'Greenleaf & Kemp Submissions on Discussion Paper')

[5] Attorney-General's Department (Australia) *Privacy Act Review Report*, December 2022 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report >

proposals in the *Privacy Act Review Report* therefore do not deal with enforcement in a systematic way.

The Attorney-General is accepting further submissions on the recommendations in *the Privacy Act Review Report* by 31 March 2023.

Purpose of this submission

Since I have previously made submissions on many of the recommendations in the Discussion Paper, there is little useful to be gained by my repetition of them. The main problem with both the Discussion Paper, and the Review Report, is that the recommendations made do not distinguish those that are useful and supportable, but only of modest effect, from those that are essential if there is to be real reform of the *Privacy Act.* These are reforms which will force data processors to change their business practices and business models (and their equivalents in the public sector) for the benefit of privacy protection.

The key to the success or failure of this reform of the *Privacy Act* is that it maintains its focus on those reforms that are essential to change business and government practices, and does not allow them to be lost in the confusion of discussing the remaining multitude of proposed reforms.

Proposals which it is most important to enact

This Submission therefore concentrates on identifying the reform proposals that should be the focus of changes to the Privacy Act (marked 'Enact' or 'Do not enact'), coupled with a brief statement of why they are so important. The order of proposals in the Review Report is followed. For those proposals I do not discuss, I support and endorse the submissions made in the Salinger Privacy Submission.[6]

4. Personal Information

It is necessary to have the broadest reasonable definition of 'personal information' and 'sensitive information', otherwise the Act will be continually avoided by technological and social changes.

Enact with amendments **Proposal 4.2** *'Include a non-exhaustive list of information which may be personal information …'.* This list should be as detailed as possible, and it should state that its purpose is to list information which makes persons 'reasonably identifiable' (see also Proposal 4.4).

What is also needed, and I submit should be enacted, is to **expand the definition of 'personal information'** so that 'identifiability' includes the capacity for 'individuation' or 'interaction' without requiring individual identification. This involves going beyond 'reasonably identifiable'. This could be found in the Discussion Paper's expansion of 'personal information' to cover circumstances in which an individual is distinguished from others'.[7] The

[6] Available from https://www.salingerprivacy.com.au/privacy-reforms/

[7] Greenleaf & Kemp Submissions on Discussion Paper: 'We propose expanding 'identifiability' to include capacity for **'**individuation' or 'interaction'**.** The DP states that the new definition 'would cover circumstances in which an individual is distinguished from others …'.[7] Salinger Privacy correctly argues that 'this is a very important and positive development, to help address the types of digital harms enabled by individuation – that is, personally targeted advertising or messaging, and personalised content which can cause harm, but which currently escapes regulation because organisations can claim that they don't know who the recipient of their messaging is.' Salinger refers to this expanded set of personal information as enabling 'individuation'. We suggest it is more understandable to refer to information which enables 'interaction' which differentiates individuals, even though

OAIC has framed this as "An individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identify is not known,"

Enact **Proposal 4.3** *'Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.'* The increasing importance of generative AI makes the inclusion of 'generated information' even more significant, but also highlights the importance of the definition of 'personal information' not being tied to identification (see above).

Enact **Proposal 4.4** *" 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment."* However, 'identifiability should no longer be the sole criterion for 'personal information' (see above).

Do not enact **Proposals 4.5 - 4.8** Enact with modifications *'Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context'* (**Proposal 4.5**) by adding 'or is capable of being distinguished from all others, even if their identify is not known'.

There is no need for a new category of 'de-identified information' (Proposals 4.5 – 4.8), intermediate between 'personal information' and 'anonymity'. This will impose lower but complex protective obligations on APP entities It is likely to be open to abuse because the protections in **Proposal 4.6** will not prevent any secondary uses of personal information, or disclosures within Australia. No separate rules are needed. 'De-identified' information is simply not 'personal information', provided the process in Proposal 4.5 is adhered to.

Enact with modifications **Proposals 4.9 & 4.10** to amend the definition of sensitive information to include 'genomic' information, inferred sensitive information and geolocation tracking data. Proposal 4.9 (c) should also expressly clarify that inferred sensitive information can be generated from information which is not sensitive information (as with inferred sensitive information).

6 - 9. Small business, employee records, political and journalism exemptions

These proposals to remove exemptions are essential to give Australia an internationally respectable data privacy Act, but they are too weak and fragmentary. The European Union, in the GDPR, has found no need for these categories of exemptions, and Australia should not do so either. A better approach should be found, either by categories of legitimate processing (as in the EU), or in some cases (eg journalism) by public interest defences. I endorse the proposals in the Salinger Privacy Submission as to how this can be done.

10. Privacy policies and collection notices

Enact with modifications **Proposal 10. 3** *'Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed…*' However, economy-wide (and society-wide) consistency, not sectoral

it does not allow them to be identified. We agree with Salinger that expanding the meaning of 'personal information' to include this capacity to individuate or interact is essential to the future effectiveness of data privacy laws.

customisation, should be required, because variability in such information is primarily used to confuse customers and citizens.

11. Consent and privacy default settings

Enact **Proposal 11.1** *'Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.'* Enact **Proposal 11.3** *'Expressly recognize the ability to withdraw consent, and to do so in a manner as easily as the provision of consent.'*

Enact with modification **Proposal 11.4** *'Online privacy settings should [be required to] reflect the privacy by default framework of the Act.'* This is not strong enough. It should require 'privacy by default', as in the GDPR, meaning that it should be compulsory that that privacy settings provide in default the maximum amount of privacy protection.

12. Fair and reasonable personal information handling

Instead of 'lawful grounds for processing' (as in the EU), it is proposed that processing in Australia 'must be fair and reasonable in the circumstances'. It is too late in this reform process to propose going down the EU route, so we must adopt the 'fair and reasonable' approach and improve it as much as possible.

Enact with modifications **Proposal 12.1** *'*... require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances … an objective test to be assessed from the perspective of a reasonable person.' This proposal is defective because it does not specify that a Commissioner or Court must be able to find, on an objective test applied by a reasonable Australian, that the if whole purpose of a 'collection, use and disclosure' is not 'fair and reasonable' by our standards, the test has not been satisfied. For example, on the approach suggested, a proposed use of facial recognition technology, or a method of individually targeted marketing, may simply be made illegal here, irrespective of how 'fair and reasonable' a way in which it is carried out, where the whole objective is not 'fair and reasonable'. This must be made explicit (perhaps as part of Proposal 12.2).This change is very important, because the value of the 'fair and reasonable' test will be reduced greatly if it is not made more robust in this way.

Enact with modifications **Proposal 12.2** *'In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: …[8 factors listed].'* This is a partial definition of 'fair and reasonable', and is a reasonable set of factors to start with, but all these factors should be included in the Act, and not only in the EM. The additional factor suggested above should also be added.

Enact with modifications **Proposal 12.3** *'The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained ….'*. It must be made clear that this does not mean that the 'fair and reasonable' test is an alternative to satisfying a requirement of consent; it is an additional requirement to consent. This is essential because it means that the Act will not be 'consent-based', but instead based on 'fair and reasonable' conduct.

13. Additional protections

Enact **Proposal 13.1** *'APP entities must conduct a Privacy Impact Assessment [prior to] activities with high privacy risks' [defined as one that is 'likely to have a significant impact on the privacy of individuals'].* 'OAIC guidance' on the meaning of 'likely to have a significant

impact on the privacy of individuals' is not strong enough. The better approach (as in Proposals 4.2 and 4.4) is to have a non-exhaustive statutory definition, so that there is a non-arguable starting point that courts can interpret. 'OAIC guidance' can be supplementary, if needed.

Enact with modifications **Proposal 13.1 '(b)** *An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.'* It is ridiculous that no one other than the OAIC should be able to require production of a PIA. Any party should be able to so require, and if the entity considers it is not an activity with high privacy risks, it should be required to demonstrate this to the OIAC (or be in breach of the Act).

13.2 Regulation of high risk biometrics and **13.3 Guidance on specific high-risk practices**

In the Discussion Paper, nine 'high privacy risk' activities' are listed as **'restricted and prohibited acts and practices'[8],** but the DP does not propose that any of them should be prohibited, but only treats them as 'restricted'. The DP proposed two options for control of restricted practices: (i) Controllers must take reasonable steps to identify privacy risks and implement mitigation measures; or (ii) Individuals are to have increased capacity to 'self-manage' these risks, by (a) consent; (b) 'absolute opt-out rights'; or (c) mandatory explicit notice. While both proposed options are two weak,[9] the DP was nevertheless considering proposals for direct intervention in far more 'high privacy risk' activities than just 'direct marketing, targeting and trading' (Proposal 20).

The Proposals avoided imposing any extra restrictions, being limited to possible PIA requirements and OAIC guidance, while the Review Report notes that many of these high risk practices are already being prohibited overseas.

This very weak response to prohibition of dangerous practices makes it even more important that the interpretation of 'fair and reasonable' practices must explicitly include the option, where necessary, of finding that whole of a practice is not, and cannot be, fair and reasonable (see **Proposals 12.1-12.2**).This would allow the prohibition of practices to grow on a case-by-

[8] Direct marketing, including online *targeted advertising* on a large scale
The collection, use or disclosure of *sensitive information* on a large scale
The collection, use or disclosure of *children's personal information* on a large scale
The collection, use or disclosure of *location data* on a large scale
The collection, use or disclosure of *biometric or genetic data*, including the use of facial recognition software
The *sale of personal information* on a large scale
The collection, use or disclosure of personal information for the *purposes of influencing individuals' behaviour or decisions* on a large scale
The collection use or disclosure of personal information for the *purposes of automated decision making* with legal or significant effects, or
Any collection, use or disclosure that is *likely to result in a high privacy risk* or risk of harm to an individual.

[9] Greenleaf & Kemp Discussion Paper Submission:'Whichever option is legislated, it will be woefully inadequate to protect privacy in relation to these nine highly contentious practices. Both 'restriction' options, if put in legislation, will impliedly legitimate some practices which it can be argued should be prohibited (perhaps with carefully controlled exceptions), such as (i), (v), (vi) or (vii) above. The Privacy Commissioner is not proposed to have a clear role in controlling practices, although the issuing of guidelines specifying practices that the Commissioner considers would not meet the 'fair and reasonable' test is suggested.[9] In the EU and elsewhere it is not yet clear that some of these acts and practices will be allowed at all, and Australia should not surrender in advance.

case basis, with appropriate limitations, rather than being set out in advance by statute. No doubt some prohibitions would be codified by statute in due course.

The Proposals **should impose direct restrictions** on more high privacy risk activities than they do at present.

15. Organisational Accountability

Enact with modifications **Proposal 15.1** *'An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.'* This proposal does not, but should, make it clear that the secondary purpose must also satisfy the 'fair and reasonable' test, otherwise there would be no restrictions on secondary use.

18. Rights of the Individual

The proposed rights of erasure, correction and de-indexing are 'rights' because refusals by APP entities can result in complaints to the OAIC (or direct enforcement), and remedies or penalties can follow. They are all necessary to bring the Act to international standards.

Enact **Proposal 18.3 Erasure** *'Introduce a right to erasure…'*

Enact **Proposal 18.4 Correction** *'… extend the right to correction to generally available publications online over which an APP entity maintains control.'*

Enact **Proposal 18.5 De-indexing** *'Introduce a right to de-index online search results containing personal information' … 'The right should be jurisdictionally limited to Australia.'* This 'right to be forgotten' is now well-accepted in Europe, and many other jurisdictions, and is distinct from either erasure or correction, so it is necessary to include it. The jurisdictional limit, properly framed, can be reasonable as it means that Australia is not attempting to legislate for the rest of the world.

Response [to exercise of rights]

Enact **Proposal 18.7** *'Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.'* The combination of notice at collection, notice in privacy policies, requirement to provide assistance in exercise of rights, and obligation to reply (Proposals 18.7- 18.10) are very desirable but must be accompanied by the OAIC being required to exercise its powers to make a determination on the complaint, in contrast to the current Act which provides in section 41 numerous avenues by which the OAIC can refuse to do so, and very often does.

19. Automated decision making

Enact with modifications **Proposal 19.3** *'Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.'* This proposal is inadequate because: (i) Notice that automated decision-making is occurring is largely useless if provided only in privacy policies; it must be

provided at the point of collection of personal information, consistent with Proposal 18.7; (ii) Notice of the right to 'request meaningful information' must occur in the same way; and (iii) The right to 'request meaningful information' should include explanation by a person, and the right to ask questions, with a right to complain to the OAIC if the explanation is insufficient.[10]

20. Direct marketing, targeting and trading

Enact with modifications **Proposal 20.1 definitions** by first ensuring that all three definitions apply to personal information which includes information where an individual may be singled out and acted upon even if their identify is not known (as in **modified Proposal 4.2**).

Enact with modifications the **first part of Proposal 20.2** *'Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for* ***direct marketing*** *purposes'.* An 'ability to opt out' is largely useless if it has to be exercised separately in relation to each marketing organisation, as distinct from just being exercised once. Where individuals wish to do so, such a 'blanket opt out' can be achieved by the enactment of (a) a 'do not direct market' central list which marketers must consult, or (b) mechanisms which individuals can adopt to automatically signal that they require an opt out from all marketing, such as has been done in Californian legislation. Such mechanisms should be enacted

Do not enact the **second part of Proposal 20.2** … *'Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.'* There is no justification for entities retaining an unrestricted ability 'to collect personal information for direct marketing without consent', because this means they can ignore the fundamental change in the reformed Act, the 'requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances' (Proposal 12.3). This amounts to a presumption that collection for direct marketing is 'fair and reasonable' which is rebuttable only by the exercise of an opt out. This is a capitulation to the most important principle of 'surveillance capitalism', the right of entities to collect personal data without consent. This provision should not be enacted at all.

Enact with modifications **Proposal 20.3** *'Provide individuals with an unqualified right to opt-out of receiving* ***targeted advertising****.'* As above, this opt-out will be largely useless if it has to be exercised separately in relation to each marketing organisation. Targeting individuals must still be 'fair and reasonable' in the circumstances (**Proposal 20.8(a)),** which provides some control (which the opt-out will not).

Enact only with substantial modifications **Proposal 20.4** *'Introduce a requirement that an individual's consent must be obtained to* ***trade*** *their personal information.'* This requires a positive 'opt in' and is fundamentally different from the previous two proposals. It is necessary to amend the definition of 'trading' so that it does not apply to make trade in personal information either a primary purpose or a related secondary purpose (see Salinger Privacy Submission for an alternative approach).

[10] Greenleaf & Kemp Submissions on Discussion Paper: 'Although the GDPR (art. 22) is defective in limiting its rights to 'decisions based *solely* on automated processing', the rights provided to individuals are significant: to obtain human intervention by the controller; to express their point of view; to contest the decision; and to have additional protections for the use of sensitive information in ADM.'

The detailed text accompanying Proposal 20.3 says that "*Where consent to trade in personal information was made a condition of accessing goods or services, an APP entity may need to demonstrate that the trading of personal information is reasonably necessary for its functions or activities if an individual objected to their personal information being traded (refer Chapter 18). while consent will be required for organisations to trade in personal information, where this is so a 'consent' to trade in personal information could be 'made a condition of accessing goods or services' so long as 'the trading of personal information is reasonably necessary for (the organisation's) functions or activities'*." In other words, the Report says that forced or bundled consent will be acceptable, when a business wants to disclose personal information for a 'benefit, service or advantage' (trading). Such trading must be 'reasonably necessary for [the business's] functions or activities', but this is just to say that it is in the business of trading information (perhaps among other businesses). Legislating to allow for the concept of 'forced consent' is the direct *opposite* of what the ACCC recommended. Proposal 20.4 (read in its entirety including the text accompanying Proposal 20.3) would effectively legitimise an industry of trading in personal information, based on forced consent, in a way that is arguably *unlawful* today. So this proposal is going to make existing problems much worse.[11] Proposal 20.4 should not be enacted unless forced consent is removed, in which case it should then be enacted.[12]

21. Security, retention and destruction

Massive data breach incidents are made far worse by disproportionate retention policies, which are sometimes encouraged by unbalanced legal provisions.

Implement with modifications **Proposal 21.6 '***The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.'* Entities should be required in relation to retention periods to implement principles of 'data minimisation' and 'privacy by default'.

Enact with modifications **Proposal 21.7 '***Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.*' Entities should be required in relation to retention periods to implement principles of 'data minimisation' and 'privacy by default'.

23. Overseas data flows

Enact in part **Proposal 23.2** *'Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).*' This proposal should only be enacted in relation to countries. There are no certification schemes which provide substantially similar protection to Australian law (and particularly not APEC CBPRs or the non-existent 'global CBPRs').

Enact with modifications **Proposal 23.3** *'Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities*.' SCCs

[11] For further argument to this effect, see the Salinger Privacy Submission.
[12] For a detailed critique of Chapter 20, see the Katharine Kemp Submission.

are an accepted global mechanism for inter-company transfers of data. However, the Act should require that any SCCs approved by the OAIC (which should be the only type possible) must provide 'substantially similar protection to the APPs'.

Enact with modifications **Proposal 23.4** *'Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure*.' 'May not apply' is a useless and weak standard of disclosure and should be replaced by a requirement (at risk of breaching the Act) to specify accurately whether the laws of the recipient's countries provide 'substantially similar protection to the APPs', and if not, why not.

Enact with modifications **Proposal 23.5** *'Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.*' APP entities should also be required (at risk of breaching the Act) to specify accurately whether the laws of the recipient's countries provide 'substantially similar protection to the APPs', and if not, why not.

22. Controllers and processors of personal information

Do not enact **Proposal 22.1** *'Introduce the concepts of APP entity controllers and APP entity processors into the Act.*' This bad and unnecessary idea would be detrimental to entities (complexity in administration and increased compliance costs) and to consumers (confusion in understanding an already over-complex Act, likelihood of utilising wrong provisions). Having a single set of obligations for all entities processing personal information is an advantage Australia's law has over many other countries.

24. CBPR and domestic certification

Implementation of 'Nil proposals' is the correct response to these two bad ideas. They should not be enacted or implemented.

25. Enforcement

Because of the enactment of the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* in December 2022, the Review Report's proposals are fragmented.

Enact **Proposal 25.2** *'Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: [factors (a) – (f) specified].'* This unused section of the Privacy Act will benefit from this greater clarity, but might still be little used because of the much higher civil penalty provisions already enacted.

Enact **Proposal 25.4** '*provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General*'. Whether or not the Commissioner already has some such powers, it will sometimes take the imprimatur of the A-G to get the Commissioner to act. This is therefore useful as an alternative to (not as a substitute for) the Commissioner's powers to undertake own-motion investigations. These powers must be retained and protected, irrespective of what the A-G may direct.

Enact **Proposal 25.5** *'Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss*'. It is important to make the ability of complainants to obtain compensation as explicit as possible.

Enact with amendments **Proposal 25.9** '*Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41*.' This is very important because section 41 is open to abuse by the OAIC using it to dispose of the vast majority of complaints under the multitude of excuses available in the various sub-provisions of section 41. This means that only a very small percentage of complainants actually receive a decision ('determination') under section 52 or reach a genuine voluntary settlement with the other party. **Proposal 25.9** should be amended to allow a complainant to require the Commissioner make a determination under section 52 – which they cannot do at present, under any circumstances. At present, there are so few determinations that almost no-one has the right to appeal against a determination. Increasing the number of appeals will mean that there is more judicial and quasi-judicial interpretation of the *Privacy Act*, which will be of great benefit to complainants, respondents and law reformers alike.

26. A direct right of action

Enact with modifications **Proposal 26.1 '***Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy.'* No matter what improvements are made to the operation of the OAIC, it will remain inadequate to enforce the numerous provisions of the Privacy Act. Unless individuals (and classes of individuals) can go directly to the courts to seek interpretation and enforcement of its provisions, dissatisfaction with the OAIC – and often complete rejection of its utility - will continue. The OAIC aims to resolve complaints without them going to court, and so there are only a negligible number of cases interpreting the Privacy Act after more than 30 years. The combined effects of the direct right of action, and the statutory tort, may change the Privacy Act from being a 'black hole' of ignorance to one with increasingly shafts of light illuminating its interpretation. They are also likely to act as a form of 'regulatory competition', encouraging the OAIC out of is litigious slumber. Consumers and citizens can only benefit.

Proposal 26.1 should be amended:

(i) The so-called 'gateway requirement' requiring complainants 'to first lodge a complaint with the OAIC before applying to the courts' is unnecessary and counter-productive, because the direct enforcement option is designed for complainants who are willing to risk costs against.

(ii) Complainants should be able to go directly to the Federal Court or the FCFCOA (depending on the size of the claim), and should be guaranteed by the legislation the right to utilise the FCFCOA's 'small claims' jurisdiction.

27. Statutory Tort

Enact **Proposal 27.1 '***Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.'* This was the best option recommended in the Discussion Paper. It is a completely different reform from the (equally necessary) Proposal 26.1 because it allows courts to find tortious breaches which are outside the Privacy Act's

restriction to 'an interference with privacy' (essentially, breaches of the APPs and its equivalents). Proposals 26.1 and 27.1 are not alternatives, but are each necessary and different ways to expand the role of the courts in creating and enforcing privacy law. The statutory tort is also likely to require courts to determine whether some acts fall within breaches of the Privacy Act, or do not but may still be serious invasions of privacy.

Author information

Graham Greenleaf AM is Professor of Law & Information Systems at UNSW Sydney where he has researched and taught the relationships between information technology and law since 1983, including intellectual property law, cyberspace law, and the development of computer applications to law. He has degrees in Arts and Law from the University of Sydney, and is a Fellow of the Australian Computer Society, and a Member of the Australian Academy of Laws. In 2010 he was made a member of the Order of Australia (AM) for his contributions to advancing free access to legal information, and to the protection of privacy.

He has been involved in privacy issues since the mid-1970s, including as a statutory Member of the NSW Privacy Committee, and an Advisor to the federal Privacy Commissioner. His *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), is a study of privacy and data protection in all 28 countries in Asia, the only study of its kind. He is Asia-Pacific Editor for *Privacy Laws & Business International Report*, which has published seven Global Survey of Data Privacy Laws by him. Over 100 of his articles on privacy are on the free access academic website, *Legal Scholarship Network* (LSN-SSRN), on which he is currently the 13th most downloaded author in the world. He is the founder of the *Asian Privacy Scholars Network*, and a board member (and co-founder, 1987) of the *Australian Privacy Foundation*. He has completed seven consultancy projects for the European Commission, advising on the level of privacy protection provided in various Asia-Pacific countries, up to 2018. He represents the Australian Privacy Foundation on the Consultative Committee of the Council of Europe's data protection Convention 108+.

In 2018 he was invited by the European Commission to be a speaker at the 'launch' of the EU's General Data Protection Regulation (GDPR). In 2021 he was a member of a consultancy team appointed by the Commission to advise on 'adequacy' applications under the GDPR. In 2022 the Council of Europe appointed him to be co-consultant on the design of a data protection law for a Pacific Island country.