SalingerPrivacy

We know privacy inside and out.

Submission in response to the *Privacy Act Review - Report 2022*

Australian Government, Attorney-General's Department

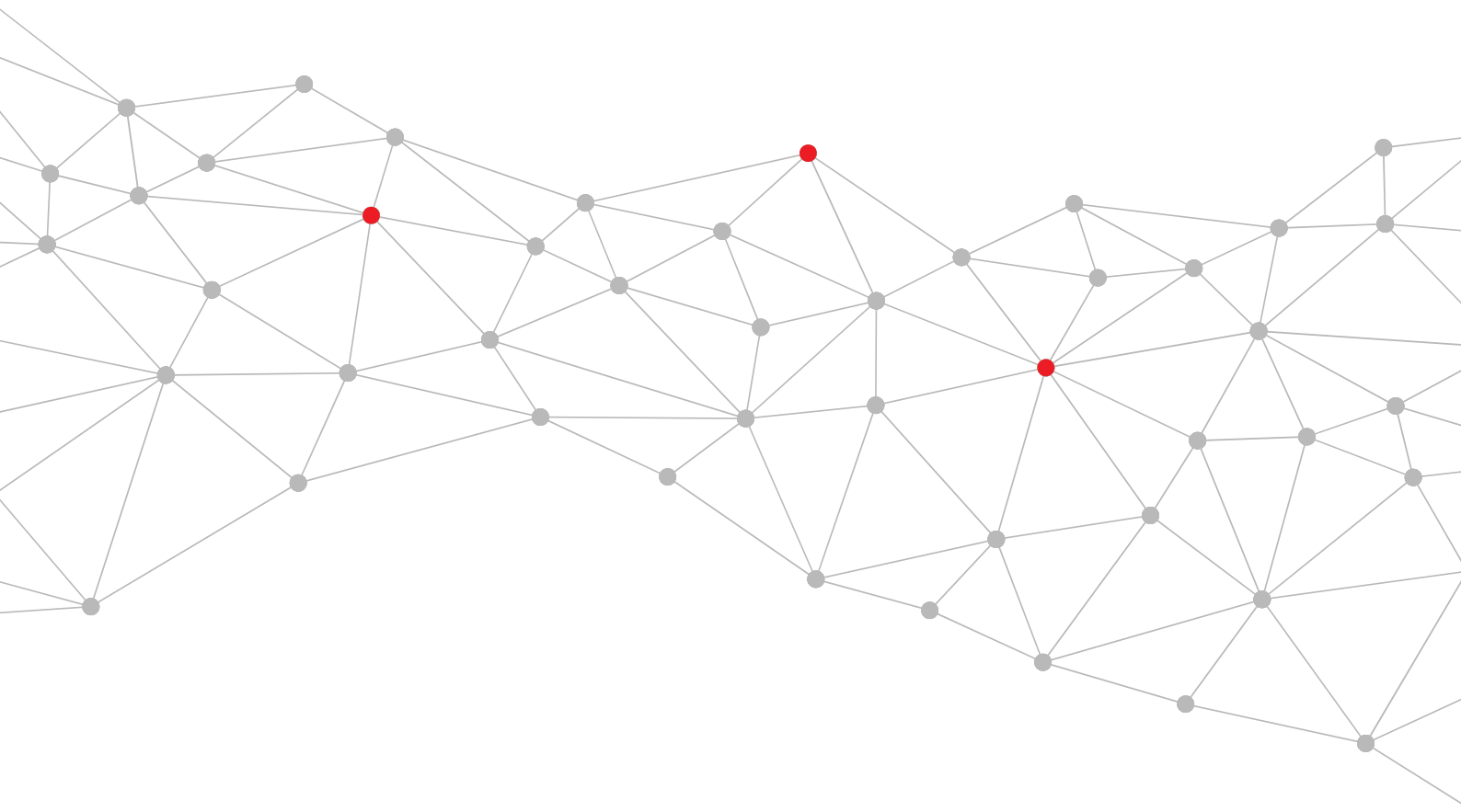
31 March 2023

Salinger Consulting Pty Ltd

ABN 84 110 386 537

PO Box 1250, Manly NSW 1655

www.salingerprivacy.com.au



Covering letter

31 March 2023

Attorney-General's Department
4 National Circuit
BARTON ACT 2600
By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: Review of the Privacy Act 1988

Thank you for the opportunity to make submissions in relation to the review of the *Privacy Act 1988*.

Please find our submission attached.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Please do not hesitate to contact me if you would like clarification of any of the comments made in this submission.

Anna Johnston
Principal | **Salinger Privacy**

Introduction and overview position

We welcome the release of the Privacy Act Review Report (the Report) and recognise its important role in modernising Australia's privacy laws. We strongly support the stated objectives outlined in the Report, particularly:

- deliver on Australian's expectations of greater protections, transparency and control over their personal information,[1]
- better align Australia's laws with global standards of information privacy protection,[2]
- enhance cross border data flows with Australia as a trusted trading partner, and have resultant economic benefits for Australian businesses and the economy,[3]
- maintain flexibility in the Privacy Act (the Act) by retaining its principles-basis,[4] and
- enhance clarity[5] while minimising compliance burden.[6]

In addition to the objectives set out in the Report itself, we are very aligned to the broader statements the Attorney-General has publicly made on the review process, including "[f]or too long, we've had companies solely looking at data as an asset that they can use commercially… We need to have them appreciate very, very firmly that Australians' personal information belongs to Australians. It's not to be misused, it absolutely has to be protected… And if the Privacy Act is not getting us those outcomes, then we need to look at reforms to the Privacy Act."[7]

We know the privacy and related harms that can arise from information handling practices which are unfair, opaque, intrusive or insecure. We know where the weaknesses in the current legal regime are. We know what the community expects. Now is the time for the Australian Government to deliver on the promise of meaningful reform.

However, we are concerned that without changes, some of the proposals in the Report will not, in practice, achieve these crucial objectives – and may even run *counter* to them.

Our first concern is that several proposals undermine the technologically neutral and principles-based approach of the Act, an approach which would lead to the Act becoming quickly outdated. We have provided examples in our submission in relation to the definitions of personal information (Chapter 4) and consent (Chapter 11), as well as the

[1] The Hon Mark Dreyfus KC MP, 'Landmark Privacy Act Review report released' https://ministers.ag.gov.au/media-centre/landmark-privacy-act-review-report-released-16-02-2023
[2] Privacy Act Review Report 2022, p. 1.
[3] Privacy Act Review Report 2022, p. 1.
[4] Privacy Act Review Report 2022, p. 2.
[5] Privacy Act Review Report 2022, p. 2.
[6] This was a recurring theme in the Report, for example see p. 2, 4, 46, 57.
[7] David Crowe, 'Voters back tougher privacy rules, penalties to protect personal data' https://www.smh.com.au/politics/federal/voters-back-tougher-privacy-rules-penalties-to-protect-personal-data-20221011-p5bowf.html?btis=

approaches to regulating direct marketing, targeting and trading (Chapter 20). Our submission offers suggestions to better future-proof the legislation, so that the Act can not only address the challenges of today, but can flex to accommodate the regulatory challenges of tomorrow. In particular, we submit that, instead of drafting provisions focusing on specific current harms (such as targeting or trading), the Bill to result from this review should instead focus on principles which would not only capture these harms, but would continue to protect Australians as practices inevitably evolve in the future to a degree which would mean they would otherwise fall outside the scope of the Act.

A further concern is that, unless this opportunity is seized to build precise and robust definitions into the Act itself, any lack of clarity will result in an increased compliance burden for organisations, as they struggle to understand their obligations. In some sectors, we would expect to see a minefield of legal arguments as companies race to the bottom to exploit any inconsistencies or 'wriggle room' in the Act, for as long as possible. This will particularly be the case in relation to the definition of 'personal information' which needs modernising, the elements of consent, and the handling of de-identified information.

This is highlighted by the recent court appeals made by Facebook Inc on the Cambridge Analytica matter in relation to the interpretation of 'carrying on a business in Australia': the companies that seek to take advantage of a lack of clarity in definitions or overarching principles generally have significant legal resources to pursue these matters, thus hampering the OAIC's ability to effectively enforce the Privacy Act.[8] As such, a key theme running through our submission is a need to ensure the Act has robust definitions that are contained in the body of the legislation itself, rather than spread across a patchwork of interpretive exercises to be performed between the Privacy Act, the Explanatory Memorandum, Codes and OAIC guidance.

Unfortunately, a number of proposals in the Report will, in our view, make the legislation less clear, and implementation more complex, thus unnecessarily increasing the compliance burden on regulated entities. The attempt to set standards for not only how 'personal information' is handled, but also how 'de-identified' and 'unidentified' information is handled, is one such example. In our submission, this will cause angst and confusion for the business community and government alike. It will also remove one of the benefits of the current legislative scheme, which is the simplicity of explaining to regulated entities that if their data meets the definition of 'personal information', they must follow a single set of privacy principles.

Additionally, we are concerned that the proposed individual rights will not live up to community expectations in terms of giving individuals control over their personal information. Our submission suggests changes to the proposals to ensure community expectations can be meaningfully met with individual rights that extend beyond the

[8] Noting the Commissioner had to make an application to the High Court to revoke Facebook Inc's special leave to appeal. While the application to revoke special leave was ultimately granted by the High Court (https://www.oaic.gov.au/updates/news-and-media/high-court-clears-way-for-oaic-case-against-facebook-to-proceed), the fact that definitional matters can end up in layers of appeals before substantive matters are even put before the courts, illustrates the potential of unclear definitions to hamper enforcement activity.

provision of notices or other information to individuals. We submit that unnecessary compliance burdens to APP entities can be avoided if proposals are prioritised according to impact to individual rights. For example, we suggest de-scoping some of the proposals, such as the introduction of a distinction between data controllers and data processors, or the requirement to publish retention periods, which we foresee having significant administrative impacts on APP entities while providing little benefit to individuals. Instead, we submit that effort should be made to broaden and strengthen the impact of the privacy principles, to better guide responsible organisational behaviour when handling the personal information of Australians.

In other words, we encourage the government to legislate for meaningful regulatory outcomes for Australians, without generating unnecessary compliance burdens for regulated entities.

Finally, we submit that the decision to either delay, further consult on, or conditionally retain the existing exemptions to the Act (small business, employee records, political parties, media organisations) is a missed opportunity to aim for 'adequacy' when measured against the GDPR and the expectations of our other trading partners. Not only are we concerned that this will impact on Australia's ability to maximise the economic benefits of this historic law reform opportunity, it will also fail to lift the compliance burden currently facing Australian businesses wishing to enter or interact with international markets.

Based on our extensive experience interpreting and applying the Privacy Act in relation to the information handling practises of government agencies, businesses and not for profit entities, of all sizes and across multiple sectors, we have laid out detailed reasoning to support our position in response to the proposals in the Report.

The table below offers an at-a-glance summary of our position. Where no additional reasoning has been provided in the body of our submission, the position in this table should be taken as our final submission.

#	Proposal (in brief)	Position	Recommendation
3.2	Recognise the public interest in protecting privacy	Support	Implement this proposal as is.
4.1 (pt 1)	Change 'about' to 'relates to'	Support	Implement this proposal as is.
4.1 (pt 2)	Include guidance about the meaning of 'relates to'	Amend	Remove from the relevant considerations: 'the extent to which the APP entity or a third party seeks to collect and use or is likely to use information to learn about or to evaluate an individual, or to treat them in a certain way, or seek to influence their behaviour or decisions'.

4.2	List of examples	Amend	This list of examples should instead be described, in statute, as what *would* make an individual 'reasonably identifiable'. The list should also include data with a weakly-obfuscated individual identifier, data with a unique or near-unique collection of demographics, and data with enough detail about the individual to identify them.
4.3	Definition of 'collect' to include inferred information	Support	Implement this proposal as is.
4.4	Entities to make own assessment about the 'reasonably identifiable' test	Amend	Amend the definition of personal information in the statute, to add: "An individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known."
4.5	Amend definition of 'de-identified'	Support	Implement this proposal as is.
4.6	Apply some APPs to de-identified data	Amend	This proposal will not be necessary if the 'reasonably identifiable' test is defined as we recommend above. Alternatively, fix this proposal to extend to disclosures under APP 6 as well.
4.7	Criminalise re-identification	Oppose	Reject this proposal.
4.8	Prohibit re-identification by recipients	Amend	This proposal will not be necessary if the 'reasonably identifiable' test is defined as we recommend above. Alternatively, fix this proposal to avoid unintended consequences.
4.9	Sensitive information	Amend	Add to this proposal an additional protection, by removing 'that is to be used for the purpose of automated biometric verification or biometric identification' from the definition of 'biometric information'.
4.10	Geolocation tracking data	Amend	Include geolocation tracking data in the definition of sensitive information.

			Reconsider the definition of 'geolocation tracking data'.
6.1	Small business exemption	Amend	Immediately abolish the small business exemption, apply a 12 month period for small businesses to prepare before any penalties apply.
7.1	Employee records exemption	Amend	Abolish the employee records exemption but introduce limited exceptions to APPs 12 and 13.
8.1 – 8.5	Political parties exemption	Amend	Remove the political parties exemption but give tailored public interest exceptions to APPs 3, 6, 12 and 13.
8.6	OAIC guidance for political parties	Support	Implement this proposal as is.
9.1 – 9.5	Journalism exemption	Amend	Abolish the journalism exemption and replace it with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism.
10.1	Clear, up-to-date, concise and understandable collection notices	Support	Implement this proposal as is.
10.2	Matters to include in a notice	Support	Implement this proposal as is.
10.3	Standardised templates and layouts	Support	Implement this proposal as is.
11.1	Definition of consent	Amend	Revert to Discussion Paper proposal 9.1: 'consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action'. Ensure consent cannot be tied to the provision of goods and services. Recognise a very narrow contractual necessity exemption to the requirement for consent to collect sensitive information.
11.2	Consent request design	Support	Implement this proposal as is.

11.3	Withdrawal of consent	Support	Implement this proposal as is.
11.4	Accessible privacy settings	Amend	Introduce a pro-privacy by default requirement.
12.1	Fair and reasonable test	Support	Implement this proposal as is.
12.2	Fair and reasonable test matters	Amend	Include all matters in the Act itself, rather than the EM. Include vulnerability in the matters to consider. Clarify that these matters will also apply to the means of collection.
12.3 (pt.1)	Fair and reasonable test to apply even where consent was obtained	Support	Implement this proposal as is.
12.3 (pt.2)	Fair and reasonable test application to APPs 3.4 and 6.2	Amend	The fair and reasonable test should also apply to conduct authorised under APPs 3.4 and 6.2.
13.1	PIAs for high-risk activities	Amend	Ensure small businesses are captured within the requirements of this proposal.
13.2	Enhanced risk assessments for FRT	Support	Implement this proposal as is.
13.3	Practice-specific guidance for new technologies and emerging privacy risks	Support	Implement this proposal as is.
13.4	Third party collection requirements	Support	Implement this proposal as is.
14.1	Broad consent for research	Amend	Any reforms in this area should be enabled as a clear and additional alternative to consent, as a ground on which a research activity can lawfully occur. This alternative legal pathway should only be enabled once an HREC has approved that use of the lower standard is appropriate and necessary in the circumstances (e.g. creation of biobanks, longitudinal or multi-use data assets).

14.2	Research permitted without consent	Support	Implement this proposal as is.
14.3	Single exception for research without consent	Support	Implement this proposal as is.
15.2	Senior employee responsible for privacy	Support	Implement this proposal as is.
16.1	Define a child in the Act	Support	Implement this proposal as is.
16.2	Children's consent	Support	Implement this proposal as is.
16.3	Clear and understandable collection notices / privacy policies	Support	Implement this proposal as is.
16.4	Best interest of the child	Support	Implement this proposal as is.
16.5	Online privacy code	Oppose	Reject this proposal.
17.1	OAIC guidance on vulnerability	Support	Implement this proposal as is.
17.2	Supported decision-making	Support	Implement this proposal as is.
17.3	Consult on acting on financial abuse	Support	Implement this proposal as is.
18.1	Access and explanation	Amend	Rephrase to state that unless an entity has incurred actual expenses over and above the reasonable processes that APP 1.2 would require them to implement to comply with this obligation, no fee should be charged.
18.2	Objection	Support	Implement this proposal as is.
18.3	Erasure	Support	Implement this proposal as is.
18.4	Correction	Support	Implement this proposal as is.
18.5	De-indexing	Support	Implement this proposal as is.
18.6	Exceptions	Amend	Explicitly state that 'rights should always continue to operate to the extent the balancing does not weigh against it'. Clarify 18.6(c) to ensure entities don't use poor process or system design to excuse not responding to individual requests.
18.7	Notification to individuals	Support	Implement this proposal as is.

18.8	Reasonable assistance	Support	Implement this proposal as is.
18.9	Reasonable steps to respond	Oppose	Compliance should not be based on a 'reasonable steps' test.
18.10	Acknowledgement of receipt	Support	Implement this proposal as is.
19.1	ADM in privacy policies	Support	Implement this proposal as is.
19.2	Indicators of decisions with a legal or similarly significant effect	Support	Implement this proposal as is.
19.3	Right to obtain meaningful information	Amend	Include a right to obtain a human review of a decision made by automated means.
20.1	Definitions of direct marketing, targeting, trading	Amend	Amend the proposed definitions.
20.2	Direct marketing opt-out	Amend	Clarify that the right extends to uses of personal information underpinning direct marketing. Add fair and reasonable test considerations.
20.3	Targeting opt-out	Amend	In order to create proactive obligations on the APP entity (rather than reactive requirements of individuals), amend the definition of 'personal information' to include information where an individual may be singled out and acted upon, even if their identity is not known. (See also Proposal 4.4.) Operationalise this proposal by amending APP 6 to specify that targeting cannot be considered a primary purpose or related secondary purpose.
20.4	Trading	Amend	Operationalise this proposal by instead amending APP 6 to specify that trade in personal information cannot be considered a primary purpose or related secondary purpose. Specify that consent to trade in personal information cannot be tied to terms of service

20.5	Direct marketing to children	Support	Implement this proposal as is.
20.6	Targeting to children	Amend	Specify that the child must have opted in to targeting. Prohibit targeting based on any sensitive information.
20.7	Trading in the personal information of children	Support	Implement this proposal as is.
20.8	Targeting – fair and reasonable test, prohibit targeting based on certain sensitive information	Amend	Entities should be required to comply with all APPs. Amend the definition of 'personal information' to include information where an individual may be singled out and acted upon, even if their identity is not known. (See also Proposal 4.4.) Prohibit targeting based on any sensitive information.
20.9	Information about targeting	Support	Implement this proposal as is.
21.1	'Reasonable steps' to include technical and organisational measures.	Support	Implement this proposal as is.
21.2	Baseline privacy outcomes	Support	Implement this proposal as is.
21.3	Enhance APP 11 guidance	Support	Implement this proposal as is.
21.4	APP 11 requirements for de-identified information	Support	Implement this proposal as is.
21.5	Enhance APP 11.2 guidance	Support	Implement this proposal as is.
21.6	Review of retention provisions	Support	Implement this proposal as is.
21.7	Require the establishment of retention periods	Support	Implement this proposal as is.
21.8	Retention periods in the privacy policy	Oppose	This proposal creates unnecessary administration, will make privacy policies even harder to read, and shifts the burden onto individuals to understand lengthy retention schedules.
22.1	Controllers and processors	Oppose	This proposal creates unnecessary administration with no benefit to individuals.

25.1	Civil penalty tiers	Amend	The proposal should contemplate the size of the business in determining enforcement tiers and penalties, so as to not expose small businesses to fines of $50m.
25.2	Clarify 'serious' interference with privacy	Amend	For clarity, consideration (c) should include children as well as vulnerable people.
25.9	Amend the annual reporting requirements in AIC Act	Amend	Amend to allow a complainant to require the Commissioner make a determination under section 52
26.1	Direct right of action	Amend	Establish a more direct and accessible avenue to exercise this right than proceedings in the Federal Court would achieve.
27.1	Statutory tort	Support	Implement this proposal as is.
28.1	Better facilitated reporting processes for notifiable data breaches	Support	Implement this proposal as is.
28.2	72 hour notification	Support	Implement this proposal as is.
28.3	NDB statement enhancements	Support	Implement this proposal as is.
28.4	AG to permit data sharing during breaches	Support	Implement this proposal as is.
29.1	Privacy law design guide	Support	Implement this proposal as is.
29.2	Regulatory cooperation	Support	Implement this proposal as is.
29.3	Working group on harmonising privacy laws	Support	Implement this proposal as is.

While we have shared our concerns, we also recognise the many positive proposals in the Report and the impact they will have in enhancing privacy rights for individuals while ensuring businesses can realise the benefits of the responsible use of personal information.

In order to future-proof the Privacy Act to deliver better outcomes for Australians, and improved clarity for entities to assist the ease of their compliance with the legislation, we offer the following analysis for the consideration of the Attorney-General and the Australian Government.

Chapter 4: personal information, de-identification and sensitive information

We strongly support the intentions underpinning the reforms to the definitions of 'personal information' and 'de-identified' information. We agree with the Report that the Act should:

- be clear to the wide variety of readers who have to apply it,
- to be flexible enough to apply to the range of activities and information that may engage the diverse range of APP entities,
- give effect to community expectations, and
- not be overly technical, nor require expertise to interpret and apply.[9]

In seeking to achieve these objectives, we have suggested some amendments to the proposals in Chapter 4, to ensure they deliver on their intentions.

Definition of Personal Information

Proposals 4.1 – 4.4 are to:

- Change the word 'about' in the definition of personal information to 'relates to';
- Include a non-exhaustive list of information which may be personal information;
- Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information; and
- Support 'reasonably identifiable' by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

We welcome proposals 4.1 – 4.3, subject to some suggested changes as discussed below.

However, we would stress the importance of establishing clear definitions in the Act to ensure its principles-basis and technological neutrality keeps it relevant as business models, practices and technology evolve. To that end, we are very concerned about the proposed step back reflected in proposal 4.4 in the Report, compared to the proposals in the 2021 Discussion Paper. In particular, proposal 4.4 will, in our view, create confusion in the definition of personal information, become quickly outdated, and result in legal loopholes which can be exploited for both existing practices and future developments.

Further, proposal 4.4 shifts too much compliance burden onto organisations to 'do their own assessment' of what the definition means in practice.

[9] Privacy Act Review Report 2022, p. 24.

The list of examples of what may constitute personal information, as per proposal 4.2, will, unless amended, still be subject to the qualifier posed by the phrase 'reasonably identifiable' in the definition of 'personal information'. Therefore, unless the phrase 'reasonably identifiable' is defined *in the statute*, in our submission the list of examples will not overcome the existing lack of clarity about what is or is not personal information. Entities will simply continue to argue that, notwithstanding that their type of data (e.g. online identifiers or pseudonyms) is included in the list of what may be personal information, because *their* data does not 'identify' any individual – and because even data in the list that does identify an individual only *may* be personal information – it is not 'personal information'. Instead, we recommend that this list of examples should instead be described as what *would* make an individual 'reasonably identifiable'. The list should also include data with a weakly-obfuscated individual identifier, data with a unique or near-unique collection of demographics, and data with enough detail about the individual to identify them.

Fixing the 'reasonably identifiable' confusion: indirect identification, singling out, being distinguishable from others, and individuation

The Report itself, the test applied by the OAIC, recent case law, the test applied under the GDPR, the expectations of the Australian community, and the stated objectives of this review of the Privacy Act, are all aligned on one thing: all of these suggest that the statutory definition of 'personal information' should clearly incorporate data that enables an individual to be singled out and acted upon, even if their identity is not known. Therefore, it is critical that the phrase 'reasonably identifiable' should be defined in the Act itself, not in the Explanatory Memorandum or additional guidance or left to the glacial development of case law, in order to incorporate this concept.

Individuation has been used to describe the 'singling out' of a person from a crowd – a threat to privacy, autonomy and dignity.[10]

In some jurisdictions the wording of the privacy or data protection statute already *expressly* includes the concept of individuation, without referencing identification first.[11] In other jurisdictions regulatory guidance has suggested that the concept of individuation (i.e. the process by which an individual can be 'singled out' or distinguished from all other members of a group) is *implicitly* included, within the notion of 'identification'. This includes Europe[12] and Australia.[13]

---

[10] Greenleaf, Graham; Livingston, Scott (2017). "China's Personal Information Standard: The Long March to a Privacy Law". *Privacy Laws & Business International Report* (150): 25–28; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3128593

[11] See for example the 2018 *California Consumer Privacy Act* (CCPA) section 1798.140(o)(1); and further discussion in *The Definition of Personal Information*, February 2020, a Research Paper prepared by Salinger Privacy for the Office of the Australian Information Commissioner; available at https://www.oaic.gov.au/__data/assets/pdf_file/0012/1308/definition-of-pi.pdf.pdf

[12] Article 29 Working Party 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007) available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

[13] Office of the Australian Information Commissioner (OAIC) guidance, 2017, *What is personal information?*, available at https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information, and

However we remain concerned that where privacy and data protection statutes use only the word 'identification' or 'identifiability', *without further explication*, different court decisions can mean that there is not a consensus about what the definition includes.

For example, in the 2015 UK Court of Appeal case, *Vidal-Hall v Google Inc*, the Court stated that "identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others".[14] However Nadezhda Purtova has noted that other European decisions are less clear on this point.[15]

It is our strong submission that rapid advances in technologies, including artificial intelligence and facial recognition, and business practices involving probabilistic and other forms of data linkage, mean that 'not identifiable by name' is no longer an effective proxy for 'will suffer no privacy harm'.[16] The Privacy Act urgently requires updating, by *explicitly* incorporating into statute the concept of individuation within the scope of the phrase 'reasonably identifiable'.

Call it 'indirect identification', call it 'singling out', call it 'distinguishing from all others', call it 'individuation' - it doesn't matter how you describe the concept. What does matter is that the wording of the definition in the Act must be clear on the face of it that what is within scope for regulation under the phrase 'personal information' includes information where an individual may be singled out and acted upon, *even if their identity is not known*.

We are concerned that the Report may have placed too much emphasis on terminology when it came to the notions of 'indirect identification' and 'individuation', which has ultimately led to the decision to exclude 'individuation' from the definition of personal information. However, the analysis underpinning this decision indicates that 'indirect identification' as described in the Report as implicitly included in the definition of personal information, has the same meaning in practice as 'individuation'. We respectfully submit that an error in the Report as to the actual definition of 'individuation' has led to this. The Report quotes the definition of 'individuation' as including "the ability to disambiguate or 'single out' a person in the crowd".[17] However, this is then reframed quite differently (and incorrectly) as "[t]he concept of individuation as understood by the Review is where information relating to an individual reveals their characteristics and can be used to impact them even though they are not reasonably distinguishable or distinguishable from all others"[18] (our own underline added to highlight the error). This is not the intention of the

---

Commissioner initiated investigation into 7-Eleven Stores Pty Ltd [2021] AICmr 50 (29 September 2021), available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

[14] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 at [115]; available at https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf

[15] Nadezhda Purtova, "From knowing by name to targeting: the meaning of identification under the GDPR, International Data Privacy Law, Volume 12, Issue 3, August 2022, Pages 163–183, https://doi.org/10.1093/idpl/ipac013

[16] Anna Johnston, 2020, "Individuation: Re-imagining Data Privacy Laws to Protect Against Digital Harms" (electronic). Brussels Privacy Hub. 6 (24); available at https://brusselsprivacyhub.eu/publications/wp624.html

[17] Privacy Act Review Report 2022, p. 35.

[18] Privacy Act Review Report 2022, p. 36.

concept of 'individuation' at all, and in fact is the opposite of our definition. 'Individuation' is a concept which seeks to explain the ability to impact an individual precisely *because* they are reasonably distinguishable from all others, but in circumstances where their 'identity' in a legal or civil sense is not known. In this sense, the OAIC's formulation of what can constitute personal information – "an individual is 'identifiable' where they are 'distinguished from all others in a group'"[19] – is in line with our argument about what should be clearly included in the statutory definition of 'personal information'.

We know the harms that can arise from individuation. These harms are not limited to use cases such as direct marketing or online behavioural advertising, but also include surveillance, stalking, discrimination, behavioural engineering, and misinformation.[20] To ensure the Privacy Act is fit to reflect the realities of the digital ecosystem, as well as meet the challenges of the future, it is critical that the definition of 'personal information' is itself fit for purpose. A strengthened statutory definition of 'personal information' will better deliver clarity for regulated entities, align with the privacy laws of our trading partners, and meet the expectations of Australians.

To highlight our contention that 'individuation' is already inherent in the notion of 'indirect identification' as expressed in the Report, we refer to the Report's discussion of existing case law, which we would expect any proposed definitions to be in line with. The Report states "The IC's determinations in the Clearview and 7-Eleven cases discuss that, generally speaking, an individual is 'identifiable' where they are 'distinguished from all others in a group'. They do not necessarily need to be identified from the specific information being handled – an individual can be identifiable where the information can be linked with other information that identifies them or where the linkage forms an ensemble that identifies them. The test does not require that an individual's legal identity be known provided the information could be linked back to the specific person that it relates to. These determinations are reflected in current OAIC guidance"[21] (our own underline added for emphasis).

The Australian case law established in the Clearview and 7-Eleven determinations clearly incorporates individuation into the definition of personal information. As these cases were accepted in the Report itself as examples of indirect identification of an individual, it is inconsistent to ultimately conclude that individuation should be excluded from the definition of personal information.

This is further supported by a quote included in Chapter 20 of the Report: "Chris Culnane and Kobi Leins have argued that the data points that represent an individual's actions, devices, location etc. are often as effective, if not more effective, at identifying an individual

[19] Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (Clearview Determination); Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) AICmr 54 (7-Eleven Determination).
[20] For a further discussion on the harms associated with individuation, please refer to our Blog 'Big Tech, Individuation, and why Privacy must become the Law of Everything' at https://www.salingerprivacy.com.au/2022/03/22/big-tech-blog/
[21] Privacy Act Review Report 2022, p. 31.

as traditional identifiers".[22] What is described in this quote is precisely 'individuation'. By referencing this concept, the Report recognises that the Act needs to adapt to the evolving, and more precise, ways that individuals can now be identified. We submit that this is further evidence that the Report's interpretation of 'indirect identification' already includes 'individuation'.

The argument to now explicitly include the concept of individuation in the statutory definition of personal information is not merely a technicality – the Report's proposal to *exclude* it could lead to significant detrimental privacy impacts for individuals. Currently, practices such as the sharing of hashed email addresses (or similar identifiers) between unrelated entities to enrich customer profiles are able to escape regulation because they can utilise middleman data brokers or 'data clean rooms' to link customer records from unrelated companies. Companies are able to claim that no individual can be identified from the data when it is in that middle 'clean' state, thus making the practice allowable.

The Report proposes to deal with some of these practices by calling them out individually and establishing bespoke individual rights in relation to them, as set out in Chapter 20. However, this is a significant risk for the privacy rights of individuals, both now and in the future. The Report itself states that "[t]he privacy risks associated with direct marketing have changed significantly since the APPs were introduced".[23] We submit that the decision to narrowly define the risks associated with 'individuation' and create ad hoc provisions to govern only some use cases means the provisions are subject to even greater risk of becoming outdated than they would be if a principles-based approach to 'individuation' was adopted (i.e. explicitly including it in the statutory definition of personal information). Just because there are current known privacy risks doesn't mean that unanticipated privacy harms won't emerge as technology advances. We submit that the only way to capture future risks is to maintain technological neutrality in the Privacy Act, rather than play legislative 'whack-a-mole' with harms after they arise.

The potential for industry to adapt in order to escape regulation is not hypothetical. In a recent article by mi-3 on the impacts of the proposed privacy reforms, Richard O'Sullivan, VP and General Manager of InMobi ANZ, stated "The reality is that at first (iOS14.5) did have an impact in Australia … but we soon found that advertisers and tech platforms adapt, learn and leverage the proliferation of data sets available to find the consumer in different environments so we quickly made up lost ground".[24] There is no question that the upcoming reforms will drive innovation amongst impacted entities. We are not against innovation, nor do we want to stifle it. However, innovation should be regulated by the Privacy Act or it risks a race to the bottom as entities structure datasets in such ways that they evade regulation, as we see with current practice.

[22] Privacy Act Review Report 2022, p. 198.
[23] Privacy Act Review Report 2022, p. 194.
[24] https://www.mi-3.com.au/19-11-2021/geolocation-privacy-changes-could-severely-impact-out-home-mobile-attribution

The only way to ensure the Act remains relevant to emerging risks is to keep it technologically neutral and principles based. A key component of this will be to recognise 'individuation' in the definition of personal information.

We therefore strongly submit that the statutory definition of personal information should, at the very least, incorporate the position from recent case law (as already reflected and accepted in the Report), and codify existing OAIC guidance,[25] by adding the following sentence:

> 'An individual is "reasonably identifiable" if they are capable of being distinguished from all others, even if their identity is not known.'

The purpose of collection should not be relevant to defining personal information

There are several instances in the Report where the purpose of a collection is proposed to be included, or already included, in a definitional decision. In our view, the purpose of use should not be relevant to how personal information is defined – this should only be assessed when determining compliance with subsequent APPs.

For example, the approach proposed at 4.1 suggests that APP entities should have regard to several relevant considerations to be found in OAIC guidance to determine whether information relates to an individual. One such relevant consideration is the extent to which a party 'seeks to collect and use or is likely to use information to learn about or to evaluate an individual, or to treat them in a certain way, or seek to influence their behaviour or decisions'.

Not only will this proposal add to the degree of confusion and complexity for APP entities, the purpose of use should not be relevant for the definition of personal information. This type of approach will create additional loopholes for bad actors to argue their way out of the definition of personal information applying to their data in the first place.

We see this in the instance of biometric information and its current scope within the meaning of sensitive information, which proposal 4.9 opted not to change. Currently, biometric information is only considered sensitive information insofar as it is to be used for the purpose of automated biometric verification or biometric identification. As new technologies emerge, so too new uses of biometric vectors that sit outside of this definition. The example given in the Report of a photograph inaccurately captures the emerging risks of biometric information, which the Report categorised as 'negligible'[26]. We respectfully disagree.

A photo that does not have biometric vectors or markers collected from it is not biometric information and it is inaccurate to use this as an example of a low-risk collection. However, an individual's voice patterns collected for the purposes of sentiment analysis in a phone

[25] As the Report itself states, codifying OAIC guidance makes propositions 'more readily enforceable': Privacy Act Review Report 2022, p. 149.
[26] Privacy Act Review Report 2022, p. 43.

call should be treated with additional care, even if that collection is not for the purpose of verifying their identity. However, at the moment, despite the growth in the voice analysis industry, this sits in a definitional grey area.

Biometric information, regardless of the purpose it was collected for, is inherently information that the individual has little-to-no ability to change about themselves and thus should be treated with additional protections. The proposal to only recognise the collection of some biometric markers as 'sensitive', based purely on the original purpose of that collection, means that people can have their biometric markers collected without their consent (and possibly also without their knowledge) and it is then open to secondary uses in line with self-serving privacy policies. The claimed original purpose of collection should not define the protections that personal information is afforded.

As such, we submit that in both instances, not detaching the definition of personal information from the purpose of a claimed original collection is a missed opportunity to strengthen privacy protections for individuals. Proposal 4.1 should be amended to remove 'the extent to which the APP entity or a third party seeks to collect and use or is likely to use information to learn about or to evaluate an individual, or to treat them in a certain way, or seek to influence their behaviour or decisions' from the relevant considerations. Proposal 4.9 should be amended to include a proposal to remove 'that is to be used for the purpose of automated biometric verification or biometric identification' from the definition of 'biometric information'.

Where should definitional matters sit?

Proposals 4.1 – 4.4 cover key definitional matters for the Privacy Act, however, in the instance of 4.1 and 4.4 (as well as 4.2, however, it appears in that instance the list itself will sit within the Privacy Act), APP entities would be directed to non-binding OAIC guidance for matters covering the interpretation of these proposals. We submit that in order to minimise confusion and compliance burden, guidance and tests related to these proposals should sit in the Privacy Act rather than outside of it. As the Report itself states, codifying OAIC guidance makes propositions 'more readily enforceable'.[27]

In our view, putting key definitional matters and tests in guidance, rather than statute, will create more confusion, rather than simplify the approach. This will be particularly true for entities being brought into the scope of the Privacy Act for the first time, especially small businesses, that will need to seek out various sources of information to piece together their compliance requirements. The degree of compliance burden depends, in part, on the clarity of the law. For example, proposal 4.4 puts the compliance burden on entities to figure out what 'reasonably identifiable' means, instead of taking this opportunity to legislate for a clear test. This won't nearly be enough to resolve the clearly articulated problems with the current definition.

[27] Privacy Act Review Report 2022, p. 149.

We further submit that there is clear evidence that when definitional matters sit in non-binding OAIC guidance, rather than the Act itself, these are open to exploitation and debate. Practices such as sharing hashed identifiers which can then be matched to individuals' profiles on unrelated entities' platforms occur today despite *existing* OAIC guidance that "(g)enerally speaking, an individual is 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of a group… This may not necessarily involve identifying the individual by name".[28]

The result of putting key definitional matters into non-binding guidance will be only further vagueness and ongoing debate, the outcomes of which will be unenforceable. Regulated entities need consistency, certainty and foreseeability in order to develop their responsible information handling practices in a level playing field, and bad actors need clear boundaries in which to operate, to prevent the exploitation of loopholes or uncertainty.

De-identification

Proposals 4.5 – 4.8 are to:

- Amend the definition of 'de-identified';
- Extend certain protections of the Privacy Act to de-identified information;
- Consult on introducing a criminal offence for malicious re-identification of de-identified information in certain circumstances; and
- Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual.

We, in principle, support the amended definition of de-identified subject to additional clarity and guidance on the phrase 'in the current context' and what re-assessments are required. Otherwise, there may be a risk that 'in the current context' may be exploited to disclose personal information with impunity.

However, we have concerns regarding the subsequent proposals for the treatment of de-identified information, which both recognise that data de-identified to the new standard carries a re-identification risk but continue to exclude it from key protections in the Privacy Act. We have some suggested modifications to the proposals to address these concerns.

The first is that disclosures under APP 6 should be included in the list of protections at proposal 4.6. The Report states that "[i]t would undermine the protections in APP 11.1 if APP entities could simply disclose de-identified information to a partner overseas where it may be re-identified without breaching the APP"[29] is a key consideration for the inclusion of APP 8 in the proposed protections. However, the Report also states that "[i]t is estimated that less than 5 per cent of businesses actively trading in the Australian economy had an annual

[28] OAIC 'What is personal information' https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information
[29] Privacy Act Review Report 2022, p. 38.

turnover of more than $3 million"[30]. As such, disclosures to up to 95% of businesses in Australia would result in the same risk as disclosures overseas, until the small business exemption is removed. Given these risks, it would be far more effective to make the disclosing entity subject to APP 6 requirements when disclosing de-identified information.

We also submit that, if de-identified data is to be regulated as a category distinct from personal information, then the use and disclosure of de-identified information should be subject to the fair and reasonable test to further protect individuals who may be at risk of re-identification in the dataset.

However, we suggest that if the definition of 'personal information' was amended to clearly state that 'an individual is "identifiable" if they can be distinguished from all others in a group' (as discussed above in relation to Proposal 4.4), this would offer suitable protections in relation to de-identified data posing a *high* likelihood of re-identifiability, because re-identifiable data would be considered 'personal information', without creating a new compliance burden in relation to de-identified data posing a *low* or remote likelihood of re-identifiability.

We submit that this solution would address many of the risks associated with targeting systems described in Chapter 20, without needing to create ad hoc legislative provisions in relation to some use cases (thus preserving the principles-based approach of the Act), or additional regulation of de-identified data as a category distinct from personal information (thus minimising unnecessary compliance burden).

For reasons already outlined in our submission to the Discussion Paper,[31] we strongly oppose proposal 4.7.

Proposal 4.8 appears to further reinforce the fact that de-identified data, without an alteration to the test of what makes an individual 'reasonably identifiable', will still carry inherent re-identification risks. While we have no objection to the *objective* behind this proposal, the risks it aims to address would be better dealt with by including disclosures under APP 6 in the list of protections that de-identified information would be subject to as submitted above; and clarifying the definition of 'personal information' as submitted above. This is further highlighted by the fact that this proposal will not have any effect where the recipient is a small business who is not subject to the Act, which is why, in our view, the obligation to protect de-identified data should rest with the disclosing entity. Proposal 4.8 as drafted could lead to unintended consequences, for example where collaborating research institutions seek to share data for the purpose of their research. (A data controller / processor distinction will not assist.)

In our experience, de-identification techniques are commonly and sensibly applied to help protect the security of the data in transit between research collaborators, but with the intention that some form of data linking activity will then occur upon receipt, in support of the

[30] Privacy Act Review Report 2022, p. 53.
[31] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p.15.

research purpose. By effectively prohibiting re-identification activities such as probabilistic data linkage, proposal 4.8 would either bring public interest research projects to a halt, or would lead to a *lessening* of privacy protections, by creating a disincentive for organisations legitimately sharing personal information to use de-identification as a method of protecting data while in transit.

Sensitive Information

Proposal 4.10 is to recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent, and to define 'geolocation tracking data'.

We submit that this is a scenario which could be better dealt with by including geolocation data in the definition of sensitive information, rather than creating a separate carve out in the Privacy Act. This is particularly true given the largest administrative burden would sit with the collection of consent, which remains a requirement under this proposal.

In addition to this, the definition proposed for 'geolocation tracking data' should be reconsidered given the vast opportunities it creates for entities to argue that the collection, use or disclosure is a 'single instance of precise geolocation data collection relevant to the concurrent provision of a service for the duration required for that service'.[32] Given that a single collection of geolocation data could impact individual's privacy rights, the requirement that data be 'collected repeatedly over time to record movements or activity'[33] should be rethought.

Conclusion to Chapter 4 proposals

In order to legislate for better outcomes for Australians, future-proof the regulatory scheme, but also *simplify* the legislation in order to ease the effort of compliance for regulated entities, and avoid unintended consequences, we submit that:

- The definition of personal information should be amended to replace the word 'about' with the words 'relates to' (as per proposal 4.1)
- 'Collection' should be defined to include inferred information (as per proposal 4.3)
- The definition of personal information must *also* be amended to add that 'An individual is "reasonably identifiable" if they are capable of being distinguished from all others, even if their identity is not known.'

[32] Privacy Act Review Report 2022, p. 46.
[33] Privacy Act Review Report 2022, p. 46.

- The Act should include a list of examples of what would make someone able to be 'distinguished from all others, even if their identity is not known', such as online identifiers, pseudonyms etc (using the list from proposal 4.2)

Exemptions to the Act

As previously stated, we strongly support the objectives of the Report, including to better facilitate cross border data transfers, with Australia as a trusted partner, and to deliver on Australians' expectations of greater protections, transparency and control over their personal information.

However, we are concerned that the proposed reforms have not gone far enough to successfully achieve these objectives.

Internationally, when the Report is read in the context of the European Commission's submission to the Discussion Paper (noting, of course, that the European Commission will ultimately decide Australia's 'adequacy' status in respect of the GDPR), the proposals regarding exemptions fall short of what was proposed by the European Commission, which supported the removal of all existing exemptions in the Act. Where an exemption was deemed to be necessary, the European Commission proposed this could be achieved via risk-based and limited tailored exemptions from certain obligations or the balancing of competing interests, rather than exempting certain entities or activities in their entirety.[34] This view is closely aligned to our submission to the Discussion Paper.

Domestically, the OAIC's Australian Community Attitudes to Privacy Survey 2020 found that almost three-quarters of Australians feel that each of the exempt organisation types should be required to protect personal information in the same ways that government and larger businesses are required to.[35] Given the community sentiment, we echo our previous submissions and submit that the proposals in the Report in relation to exemptions must be revised if they are to bring Australia's privacy laws in line with global and community standards.

Small Business Exemption

We are concerned that while the Report proposes to remove the small business exemption, this will only be done, as some undefined point in the future, after further consultation, an impact analysis, and once small businesses are 'in a position to comply with these obligations'[36]. In lieu of this approach, we submit that the small business exemption should be immediately abolished, however, a 12 month period be applied for small businesses to prepare before any penalties apply. In addition to this, we submit that the OAIC will need to be adequately resourced to develop the support and training package immediately.

[34] European Commission, 'Consultation on the review of the Privacy Act 1988' p. 2.
[35] OAIC Australian Community Attitudes to Privacy Survey 2020, p. 60.
[36] Privacy Act Review Report 2022, proposal 6.1.

The reasons to abolish the small business exemption have been well articulated throughout this Review process. As such, we have a number of concerns in regards to the current proposals in the Report on the small business exemption.

Our first concern is that the small business sector is not homogeneous and therefore it will never be possible to meet the pre-conditions placed on the abolition of the exemption as part of this proposal, particularly the requirement that small businesses are in a position to comply with the obligations imposed by the Act.

It's important to recognise that maintaining the small business exemption in its current form, carries a compliance burden in its own right, for example in constantly negotiating cross-border rules. In addition to this, there is an economic cost associated with being kept out of competitive markets that extends to all businesses in Australia's economy wishing to engage with those markets. We submit that continuing to exempt small businesses from the Act does growing businesses no favours in the long run. If businesses are not set up properly from the start to implement 'fair and reasonable' personal information handling practices, or to only collect sensitive personal information or geolocation data with express consent, then when those businesses grow past the arbitrary $3M turnover mark they will suddenly face a compliance task which may involve re-architecting their systems and business processes, if not also their business model. In addition to this, small businesses have the compliance burden of working out in what scenarios the Act would begin to apply to them. Not having a single standard for all entities also means small businesses face a compliance hurdle when entering into agreements with APP entities, which would typically utilise contracts to oblige their partners to comply with the Act.

We submit that the proposals in the Report that aim to resolve the interim risk posed by small businesses will actually add further compliance burden, particularly in understanding the distinction between processors and controllers (and the even more complex distinction between processors and joint controllers), the complexities of sub-contractor arrangements between small businesses, and ensuring contract negotiations factor in the correct type of arrangement. Having a single rule to apply to all businesses will better address privacy risks while minimising compliance overheads for small businesses.

As we have stated in previous submissions, privacy rules already have inbuilt mechanisms[37] to ensure compliance burden is balanced against privacy risk. We submit that these sufficiently deal with ensuring risk is factored into balancing the compliance burdens individual entities face. Furthermore, leveraging existing and well established rules as the basis for OAIC guidance for small businesses will result in a far more streamlined transition for small businesses than the introduction of concepts such as controller and processor, which have not yet been tested in the Australian regulatory landscape.

Finally, we refer back to the key objective of the Report to deliver on Australians' expectations. The OAIC's Community Attitudes to Privacy Survey 2020 showed that only 15% of surveyed individuals correctly identified that small businesses are not covered by

[37] For example, APPs which require only such steps to be taken as are reasonable in the circumstances.

the Act. As the OAIC called out in the survey "[t]he low proportion of people correctly identifying which business types are not covered is consistent with a population simply assuming that most businesses are covered"[38]. Continuing to maintain an exemption for small businesses, even if this is temporary during further impact analysis (although we continue to be concerned that the pre-conditions for the removal of the exemption may never be met), is clearly not in line with community expectations on how personal information is protected. Coupled with the fact that up to 95% of Australian businesses are covered by the exemption, we again submit that the small business exemption should be immediately removed.

As such, we submit that the small business exemption should be immediately abolished, however, a 12 month period be applied for small businesses to prepare before any penalties apply.

In relation to penalties for small businesses, we submit that **proposal 25.1** should contemplate the size of the business in determining enforcement tiers and penalties, so as to not expose small businesses to fines of $50m.

On a more operational matter, we submit that small businesses should not be exempt from the requirement to conduct a Privacy Impact Assessment (PIA) for activities with high privacy risks (**proposal 13.1**). We note that the discussion on proposal 13.1 suggested that "consideration could be given to whether some small businesses that are covered by the Act, or may become covered by the Act in the future should the small business exemption be removed, should be exempted from the PIA requirement on the basis that they are less able to absorb its associated regulatory costs".[39] Proposal 13.1 is already limited to high risk activities, which inherently means any small business that is brought within its scope has met a risk threshold. PIAs are a key tool by which privacy risks can be identified and mitigated. If small businesses are exempt from conducting PIAs, they would have no structured manner in which to identify risks. We recognise that PIAs can introduce administrative workload to businesses but given the importance of PIAs as a risk mitigation tool, we submit that instead of being exempt from the requirement, small businesses are provided with short form templates to assist them in identifying privacy risks in a more streamlined way (for example, checklists based off APP guidance). This would ensure risk is effectively balanced against the associated compliance burden.

Employee Records Exemption

We echo statements made in our previous submission[40] and submit that **proposal 7.1** does not go far enough to protect employees from privacy harms.

[38] OAIC Australian Community Attitudes to Privacy Survey 2020, p. 58.
[39] Privacy Act Review Report 2022, p. 125.
[40] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p.18

We submit that the existing APP framework already incorporates the necessary balance employers require in relation to administering the employment relationship efficiently – acts done for the primary purpose of administering the employment relationship would not cause undue compliance burden for employers, and APP 6 already allows for activities that are authorised by other laws, in this instance employment laws. Furthermore, employers are already required to turn their attention to the Act in respect of their recruitment activities for prospective employees not covered by this exemption, thus they are already required to interact with the Act for personnel matters. We submit that as uses of employee personal information in the workplace evolve, for example as workplace monitoring edges more into productivity scoring (which, in addition to its intended use, can reveal even more information about employees via inference),[41] obligations need to be placed on employers to ensure the use of personal information sourced from employee records is not unfettered and that the achievement of business objectives does not come at the cost of individuals' privacy rights.

As put forward in our earlier submission, a better solution to the handling of employee records is to abolish the employee records exemption but introduce limited exceptions to APPs 12 and 13.[42]

Political Parties Exemption

The commentary in the Report stated "[a]lmost all submitters that commented on the [political parties] exemption considered that it was not justifiable".[43] We firmly agree with this view. However, proposals 8.1 – 8.5 demonstrate a disappointing shift of responsibility onto individuals in relation to interactions with political parties, particularly since individuals may have no visibility of which political parties hold their personal information, in favour of continuing to preserve the political parties exemption.

We submit that this approach is untenable. Instead of trying to retain the exemption and introducing limited obligations based on identified harms (e.g. data breaches), a better approach would be to remove the exemption but give tailored public interest exceptions to APPs 3, 6, 12 and 13. This is aligned with our earlier point that trying to anticipate harms and legislating for them will be far less effective in the long run than maintaining the principles based approach of the Act.

We have several concerns with the approach set out in proposals 8.1 – 8.5 and the detrimental impacts it will have on individuals' privacy rights:

- Proposal 8.2 shifts responsibility onto individuals to seek out privacy notices from political parties without necessarily knowing which political parties have collected their personal information. Furthermore, as individuals have no actionable rights (e.g. right to object, right to seek access) if they disagree with a political party's

[41] https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html
[42] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p.18
[43] Privacy Act Review Report 2022, p. 73.

personal information handling practices, this proposal does not meaningfully shift the status quo.

- Proposal 8.3(a) fails to meaningfully impact existing practices as it would be open to political parties to argue that all their practices are done in the interest of protecting democracy and political free speech, thus are fair and reasonable in virtually any circumstance.
- Proposal 8.3(b) does not adequately recognise that targeting based on *any* sensitive information can cause harm to individuals. Targeting inherently involves revealing sensitive information to other parties (e.g. social media companies for the purposes of advertising), who could then add this information to their own profiles of individuals. Targeting forms part of a much broader data ecosystem that should be considered in this context. When coupled with the fact that individuals may not know that a political party has even collected their personal information, those parties having the power to use and disclose sensitive information in this way would sit beyond community expectations of the protections political parties must apply to their personal information.
- Proposal 8.4 once again disappointingly shifts responsibility onto individuals to find out who has their information and then find ways to opt out of this communication, particularly since political advertising / targeting does not always make it clear who is targeting you – the ad can be against something, rather than directly for a specific party. As such, the burden on individuals is not insignificant.

In order to address these issues, meet community expectations and future-proof the Act, we submit that the political parties exemption be removed and tailored public interest exceptions to APPs 3, 6, 12 and 13 developed to ensure individual privacy rights are more fairly balanced against the continuation of political free speech.

Journalism Exemption

We submit that proposals 9.1 – 9.5 do not meaningfully change the status quo or address the privacy harms associated with the existing journalism exemption. We re-iterate the statements made in our previous submission: the journalism exemption should be abolished, and replaced with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism.[44]

The need for more robust reform continues to be evidenced in the privacy harms caused by entities relying on the journalism exemption. A recent example of these harms was illustrated by Brittany Higgins' twitter post referencing a media outlet publishing private images, texts and WhatsApp messages from her phone for a third time[45] in circumstances where the publisher of the outlet is an industry nominee member of the Australian Press

[44] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p.19.
[45] https://twitter.com/BrittHiggins_/status/1626690964365672448?s=20

Council (APC),[46] thereby making them subject to the APC's Standards of Practice (which include privacy standards).[47] We draw your attention to the fact that this highly intrusive scenario would be compliant under the proposals set out in the Report.

As such, we reiterate that proposals 9.1 – 9.5 are insufficient to protect individuals' privacy rights. We submit that a better approach would be to abolish the journalism exemption and replace it with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism.

[46] https://presscouncil.org.au/about-us/who-we-are/
[47] Privacy Act Review Report 2022, p. 85.

Chapter 11: consent and privacy default settings

Proposals 11.1 – 11.4 are to:

- Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous;
- Have the OAIC develop guidance on how online services should design consent requests;
- Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent; and
- Require APP entities that provide online services to ensure that any privacy settings are clear and easily accessible for service users.

We welcome proposal 11.3, however, we have concerns regarding the practical impact of proposals 11.1 and 11.4.

Definition of consent

As previously set out in this submission, embedding clear definitions of key concepts in the Act itself will help ensure the Act remains principles based and technologically neutral, thus minimising the risk of it becoming quickly outdated. Another such key definition is consent, which we submit was well crafted in the Discussion Paper.

While we support the intention to strengthen consent requirements, we are concerned about the step back from the Discussion Paper in relation to several key matters to do with the definition of consent, namely the exclusion of 'indication through clear action' in the definition of consent (proposal 11.1), and the creation of exceptions where it will be permissible for consent to be made a condition of accessing goods or services (proposal 20.4).

Indication through clear action

We continue to strongly support the definition of consent which was proposed in the Discussion Paper at proposal 9.1: "consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action"[48] (emphasis added) and note that this definition is consistent with recommendation 16(c) in the Digital Platforms Inquiry Final Report (DPI Report) which set out that "valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent)".[49]

[48] Discussion Paper p.11
[49] Digital Platforms Inquiry Final Report June 2019, p.35

We submit that retaining this definition is necessary to prevent the exploitation of unclear terms in the definition, so as to continue practices which undermine individuals' informed and free choices.

We respectfully but strongly dispute the suggestion that the removal of 'indication through clear action' is necessary to facilitate processes in the clinical healthcare settings, such as sending pathology samples to a laboratory.[50] Existing mechanisms in the Act, such as permitted health situations (s.16B) and the permissibility of the use and disclosure of sensitive information where that use or disclosure is reasonably expected and is for a directly related secondary purpose (APP 6.2(a)), already cover the scenario described in the Report. We further submit that the concerns about impact to medical research are equally addressed by existing mechanisms within the Act, particularly the research exemptions (ss.16B, 95 and 95A).

Reverting to the definition proposed in the Discussion Paper will help prevent ongoing privacy harms caused by entities exploiting unclear consent requirements. The ACCC called out a similar concern in the DPI report: "many businesses seek consent to data practices using click-wrap agreements, bundled consents, and take-it-or-leave-it terms where consumers are not provided with sufficient information or choice regarding the use of their personal information".[51] Given these practices exist in the current environment (which requires consent to be voluntary, informed, current and specific), there is precedent to suggest that anything short of a clear definition in the statute will result in the continuation of problematic practices to obtain consent.

As such, we submit that the definition of consent as proposed in the Discussion Paper (consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action) should be the version incorporated in the Act.

Consent as a condition of accessing goods or services

We are deeply concerned about the implications of proposal 20.4 and its ability to undermine the voluntariness of consent, namely by proposing that consent to trade in personal information can be tied to the provision of goods and services: "[w]here 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".[52]

Creating carveouts that undermine consent for non-essential and harmful activities such as trading personal information undermines the principle of voluntariness, and thus the principles-basis of the Act. We foresee this being misused by bad actors, further

[50] Privacy Act Review Report 2022, p. 104.
[51] DPI Final report p.25
[52] Privacy Act Review Report 2022, p. 214.

entrenching murky Adtech practices, and fundamentally undermining an individual's bargaining power when it comes to their personal information.

We submit that the requirement for consent to be voluntary is an existing requirement under the Act and thus should not be undermined as part of these reforms.[53] In their submission to the Issues Paper, the OAIC stated that it supports the view that "[c]onsent is not freely given when the provision of service is conditional on consent to personal information handling that is not necessary for the provision of the service".[54] This has also recently been re-iterated by the European Data Protection Board (EDPB) in its Binding Decision against Meta and the use of personal data for the purposes of behavioural advertising for its Facebook service, where several Supervisory Authorities considered that tying non-essential processing to terms of service amounts to 'forced consent': "even if Meta had relied on consent, it would not have met the requirements of… being 'freely given', as the service is conditional on the use of the Facebook service as a whole ('take it or leave it')".[55]

In its DPI Report, the ACCC raised concerns about consent tied to the provision of services and the impact this has on consumers: "[t]he ACCC also found considerable imbalance in bargaining power between digital platforms and consumers. Many digital platforms use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limit the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data".[56]

Introducing carveouts for digital platforms or loyalty schemes to tie consent to the provision of services undermines one of the ACCC's key recommendations, and arguably the *raison d'etre* of this very review.

This proposal will also further entrench the imbalance of bargaining power that the ACCC's DPI Report raised concerns over. It will also run counter to the articulation of consent in the GDPR, thus putting Australia *further* out of alignment with global standards.

The impact to consumers of this proposal will be significant – the Consumer Policy Research Centre's 2020 Data and Technology Consumer Survey of 1000 consumers found that 69% of consumers who read privacy policies reported accepting terms even though they weren't comfortable with them. The main reason for doing so was it was the only way to access the product or service (75%).[57] Specifically on loyalty schemes, a survey of 280 CHOICE members found widespread discomfort over the collection and use of their

[53] OAIC, 'Chapter B: Key Concepts' https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts#consent
[54] OAIC, "Privacy Act Review Issues Paper submission", 14 December 2020, part 5.42; available at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/
[55] European Data Protection Board, 'Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)', Adopted on 5 December 2022, para 146;
[56] DPI Final report p.23
[57] Consumer Policy Research Centre, CPRC 2020 Data and Technology Consumer Survey, Consumer research conducted in partnership with Roy Morgan Research over March and April 2020; available at https://cprc.org.au/wp-content/uploads/2022/03/CPRC-2020-Data-and-Technology-Consumer-Survey.pdf

personal information through retail loyalty programs.[58] On a scale of one to five (one being "not comfortable at all"), 61% answered one or two when asked how comfortable they are with the type of information collected about them. Even more respondents were uncomfortable with the amount collected and for how long and how securely it is stored. And 84% had concerns about with whom businesses were sharing their information.[59] As CHOICE contended, widespread ignorance of the ways customer data can be used by organisations is a boon for businesses with loyalty programs, as it allows them to trade sometimes meagre rewards and discounts for their customer's valuable personal information.[60]

We echo the concerns of the ACCC in the DPI Report and submit that allowing consent for trading to be tied to service provision entrenches power imbalances and undermines the definition of consent in the Act. By putting conditions on it for specific use cases, despite the known harms arising from those uses, the principles-basis of the Act is compromised in an unfair balance towards unjustified business interests.

We are cognisant of the fact that the Act recognises that privacy rights of individuals must be balanced against the interests of entities in carrying out their functions or activities. However, as the EDPB recently highlighted in its Binding Decisions against Meta, Meta's business model of offering services, at no monetary cost for the user to generate income by behavioural advertisement to support its services "does not make this processing necessary to perform the contract... it is the business model which must adapt itself and comply with the requirements that the GDPR sets out… and not the reverse".[61] Business models should not set regulatory priorities, particularly when they are in conflict with the public interest in privacy.

Given the harms to not only individuals in the specific instance of trading personal information, but to the overarching principles-basis of the Act, we strongly submit that consent should never be tied to the provision of goods and services and all references to this should be removed.

In contrast to instances where consent is bundled into terms of service for additional secondary uses of personal information, we do recognise instances where a service cannot be provided without the collection (including by inference) of sensitive information, for example fertility apps or a fitness class specifically for pregnancy. In these unique instances, we submit that it is still preferrable to maintain the principles basis of the Privacy Act and not undermine the elements of consent. For these very limited circumstances

[58] https://www.choice.com.au/shopping/consumer-rights-and-advice/your-rights/articles/loyalty-programs-data-collection-privacy-law
[59] https://www.choice.com.au/shopping/consumer-rights-and-advice/your-rights/articles/loyalty-programs-data-collection-privacy-law
[60] https://www.choice.com.au/shopping/consumer-rights-and-advice/your-rights/articles/loyalty-programs-data-collection-privacy-law
[61] European Data Protection Board, 'Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)', Adopted on 5 December 2022, para 119; European Data Protection Board, 'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)', Adopted on 5 December 2022, para 122.

where a service cannot be provided without the collection of sensitive information, we propose a recognition of a very narrow contractual necessity exemption to the APP 3.3 requirement to obtain consent for collection, provided that the sensitive information is collected directly from the individual. The onus would be on the APP entity to demonstrate that the collection of the sensitive information is essential to perform the primary service requested. For additional consumer protection, we submit that direct marketing, targeting and trading can never be services for which the collection of sensitive information is essential.

Privacy by default settings

We support the intention behind proposal 11.4, however, we are concerned that in its current form, the proposal will not achieve what it sets out to. We submit that the better approach remains Option 1 from the Discussion Paper on this proposal, that is, 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.[62]

While the Report suggests that existing mechanisms in the Act operating alongside a fair and reasonable will "together effectively operate as a requirement similar to Option 1 and give effect to the data minimisation principles underpinning the Act"[63] we do not believe this will be the case. This appears to be conceded in the Report when it states that privacy settings must be "clear and easily accessible for individuals to modify them, including to make them the most restrictive and privacy protective generally"[64] – if privacy by default settings were required, then individuals would not need to navigate through multiple screens on multiple websites to then apply the 'most restrictive and privacy protective' settings. Given the submissions put forward against Option 1, it is likely that APP entities will be able to argue that those settings *are* required for their business activities, and therefore the objectives of pro-privacy by default will not be realised.

We reiterate our position on pro-privacy by default as set out in our submission to the Discussion Paper: we do not believe that the self-management approach of Option 2 is sufficient, and will result in arguments about whether or not system design is utilising 'dark patterns' to direct users away from making the most privacy-protective choice, and/or whether the privacy settings are 'obvious and clear', and simple enough to be utilised. We have recently seen this continue to cause headaches in the EU where the EDPB assembled a 'cookie banner taskforce' to review the various dark pattern types still in use on cookie banners following the lodgement of over 700 complaints by privacy advocacy group NOYB.[65] We anticipate that without clear direction to set pro-privacy by default in statute, we will see similar 'dark patterns' continue to be used to ensure users do not restrict data collection practices.

[62] Privacy Act Review Report 2022, p. 107.
[63] Privacy Act Review Report 2022, p. 108.
[64] Privacy Act Review Report 2022, p. 108.
[65] See https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

Beyond this, we submit that not having strong enough privacy default settings may also mean the objectives of providing further support to people experiencing vulnerability may not be achieved – design should reflect the needs of the most vulnerable users. This proposal does not achieve that, and it may disproportionately impact vulnerable users as a result.

We submit that, given Option 2 will not achieve the same effects in practice as Option 1 (which we note was widely supported in submissions to the Discussion Paper),[66] a requirement to implement pro-privacy default settings in line with Option 1 should be introduced into the Act.

[66] Privacy Act Review Report 2022, p. 107.

Chapter 12: fair and reasonable personal information handling

Proposals 12.1 – 12.3 are to:

- Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances;
- Set out matters that entities may take into account in determining whether a collection, use or disclosure is fair and reasonable in the circumstances;
- Clarify that the fair and reasonable test will apply irrespective of whether consent has been obtained. Also clarify that the fair and reasonable test should not apply to exceptions in APPs 3.4 and 6.2.

The fair and reasonable test

We strongly support proposal 12.1 with no amendments.

We also welcome proposal 12.2, however, submit that all the factors that entities should have regard to, including those related to proportionality, should be listed in the Act, rather than the Explanatory Memorandum. Not only will this ensure it is easier to enforce the provision, it will also minimise the compliance burden for entities – it is far easier to look at one source of information than to search across multiple documents to understand the requirements of the fair and reasonable test. The proportionality test is crucial and should be set out in the Act itself.

We also submit that, in line with proposal 17.1 on uplifting privacy protections for individuals experiencing vulnerability, vulnerability should be a factor considered in proposal 12.2. The Report already suggests a mechanism by which this could be included in the fair and reasonable test: "While the 'fair and reasonable test' would be assessed objectively, where an entity is aware that it is likely to be handling information of people experiencing vulnerability, or is engaging in activities which could have a significant effect on people experiencing certain vulnerabilities, those circumstances will be relevant to whether the entity's information handling objectively satisfies the fair and reasonable test".[67] We submit that this mechanism as described in the Report should be incorporated into the list of factors at proposal 12.2.

We further submit that in light of the proposal to repeal the 'fair means' of collection rule currently in APP 3.5 (proposal 12.3), it should be made clearer to entities that the matters at proposal 12.2 also apply to the *means* of collection.

[67] Privacy Act Review Report 2022, p. 159.

Finally, we submit that there would be benefit in clarifying that *all* the factors set out at proposal 12.2 should be considered in an entity's determination. This would be to prevent entities from claiming that a practice is fair and reasonable merely because it is reasonably necessary for the functions and activities of the organisation. The requirement for a practice to be reasonably necessary for the functions and activities of the organisation already exists under APP 3 and APP 6 and thus if this was the only factor considered, it would undermine the application of this proposal. Further, 'reasonably necessary for the functions and activities of the organisation', if taken alone, can too easily be used to justify even the most invasive practices as the foundations upon which a business model rests. As such, we suggest either a prioritisation or weighting of factors, or phrasing in the test itself could guide entities towards considering all factors of the test.

Application of the fair and reasonable test

We strongly support the proposal that the fair and reasonable test be applied irrespective of whether consent has been obtained.

However, for the reasons set out in our submission to the Discussion Paper[68], we submit that the fair and reasonable test should apply to *all* instances of collection, use and disclosure, including those authorised under APPs 3.4 and 6.2.

[68] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p.22.

Chapter 14: research

Proposals 14.1 – 14.3 are to:

- Introduce a legislative provision that permits broad consent for the purposes of research;
- Consult further on broadening the scope of research permitted without consent;
- Consult further on developing a single exception for research without consent and a single set of guidelines.

Proposal 14.1 – broad consent

We support this proposal, but with the important caveat that any reforms in this area should be enabled as a clear and additional *alternative* to consent, as a ground on which an activity can lawfully occur. This is important, in order to maintain the clear guidance that, as per proposal 11.1, *consent* in all circumstances must be voluntary, informed, current, specific, and unambiguous.

We also suggest that, so as to avoid creating confusion on what constitutes a valid consent, instead of using a term such as '*broad consent'*, this alternative legal pathway should instead be described as something like '*enduring research agreement'*. Further, it should be defined that an enduring research agreement, to be valid, would still need to be voluntary, informed and unambiguous.

Further, this alternative legal pathway should *only* be for research projects, and research data asset creation, as approved by a human research ethics committee (HREC), and only once the HREC has approved that use of this alternative legal pathway is appropriate and necessary in the circumstances, such as where the consent elements of 'specific' and 'current' pose particular difficulties. Examples would include the creation of biobanks, longitudinal or multi-use data assets, or public interest data analytics centres.[69]

Otherwise, we are concerned that the proposal as drafted could allow the type of self-serving definitions of 'research' and corporate behaviour that we saw when Facebook manipulated members' news feeds in order to experiment on its members and test its theories about emotional contagion. Facebook sought to justify its conduct by claiming that its members had agreed to non-specific 'research' uses.[70]

[69] Salinger Privacy has conducted Privacy Impact Assessments of a number of large and complex enduring data linkage and data asset projects, including the ALife longitudinal data asset developed by the Australian Taxation Office, the Lumos Data Asset developed by the NSW Ministry of Health, the NSW Health Statewide Biobank, the management of the NSW Cancer Registry, Phase 1 plans for the National Disability Data Asset, models for data linkage for the NSW Centre for Health Record Linkage, the establishment of the Victorian Centre for Data Insights, and the establishment of the NSW Centre for Education Statistics & Evaluation.

[70] https://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/

We suggest that the requirement to include approval by an HREC as a pre-condition to the application of this alternative legal pathway will ensure that important privacy protections are maintained, but without unnecessarily increasing the compliance burden on either researchers or entities which hold data to which researchers are seeking access. HRECs routinely review research applications even where a research exception is not being relied upon for the personal information handling aspects of the project, because the HREC must examine the ethical implications of the project and the impact on individual privacy in any case. For example, patient information and consent forms (PICFs) are routinely reviewed by HRECs for consented studies (which do not need to rely on a s.95 or s.95A research exception to proceed) such as clinical research.

While we note that the Report suggests that research is 'usually' conducted using de-identified information or with participants' express consent,[71] in our experience this actually depends greatly on the nature of the research project or activity. What happens in clinical research involving active patient participation is vastly different to what happens in the creation of longitudinal datasets, complex data linkage activities, biobanking or the establishment of enduring data assets.

In our experience, de-identification techniques may be applied, along with other controls such as role-based access controls and ring-fencing data within a secure data enclave, as a way of minimising the privacy risks to arise from the use of personal information in research. The use of de-identification in this context is about ensuring appropriate data security, rather than seeking to escape the requirements of the Act by claiming that the data is 'de-identified' such that is not personal information in the first place. Therefore, even if the research is conducted using de-identified information, the lawful authority to conduct that research in the first place will still rely on application of a research exception to the collection, use or disclosure principles.

Proposals 14.2 and 14.3 – amend the research exceptions

We strongly agree with proposals 14.2 and 14.3, and we urge the Department to progress these proposals immediately. The current exceptions for research, currently found in sections 16B, 95 and 95A of the Privacy Act, ought to be re-considered and re-drafted, as a single new exemption to APPs 3 and 6 (and 8), with a single set of guidelines.

We agree that the scope of the two current exceptions is too narrow, and that the distinction between public sector and private sector application is an unnecessary hangover from the pre-2014 structure of the Act.

As we noted in our previous submission, currently personal information held by Australian government agencies cannot be used to conduct *non-medical* research, such as research into the financial effects for working mothers of altering childcare rebates, or research into the educational outcomes achieved by changing tertiary education funding.

[71] Privacy Act Review Report 2022, p. 133.

Meanwhile private sector organisations cannot use *non-health* personal information in research projects, even if those projects are highly relevant to public safety, such as research into better designing personal protective gear to fit the different body shapes of a workforce.

The breadth of 'research' should not be limited to 'medical research' or even 'public health or public safety'. Nor should the scope of the personal information covered by the exception be limited to health information. As the Report makes clear, important research in the public interest, which is dependent on the collection and use or reuse of personal information, can cover topics from criminology to climate change.

Further, both current exceptions fail to give due consideration to the steps preliminary or ancillary to the conduct of the research itself, such as the steps involved in participant identification and recruitment.[72]

Both current exceptions also fail to consider the increasingly common scenario in which what is being proposed or built is not a discrete collection or use of personal information for a single research project, but the creation of a biobank or significant data asset, which will in turn support multiple research projects into the future. The exceptions as drafted work on the now-outdated assumption that research is something that only ever happens as a singular or ring-fenced 'project'.

We work with many clients in the research and data analytics space, in both the public and private sectors, and we have often found the drafting of s.95 and s.95A to prohibit or constrain research that would otherwise have a high public interest value. This is one area where the federal Privacy Act lags significantly behind the privacy laws of our States and Territories, where research provisions are much more generously and sensibly drafted; they do not artificially constrain the scope of their research exemptions.

We have also witnessed what is described in the report[73] as 'conservative and incorrect decision making' which hinders the conduct of effective research, because of the difficulties for researchers (and entities holding data to which researchers want access) in understanding and applying sections 16B, 95 and 95A. We have also seen incorrect decision making which puts entities at risk of breaching of the Act, through the application of the wrong test, such as the s.95A test being applied to the release of data by government agencies.

As we argued in our submission on the Discussion Paper, the essential conditions for allowing research involving personal information to proceed should remain: i.e. that an appropriately-constituted HREC has approved of the proposed collection, use or disclosure

[72] See *'PA' and Department of Veterans' Affairs* (Privacy) [2018] AICmr 50 (23 March 2018) for an example of a case in which the OAIC had to stretch the literal meaning of s.95 to allow for the participant recruitment phase to fit within the umbrella of the research exemption; available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2018/50.html

[73] Privacy Act Review Report 2022, p. 138.

of personal information as necessary for a research project (or, in our view, and taking on board the matters noted above, the establishment of a biobank or significant data asset which will in turn support multiple research projects) which is in the public interest, the expected benefits of which outweigh the public interest in the maintenance of privacy protections. The HREC must also still be required to attest that a waiver of the requirement to gain an individual's consent is necessary (otherwise the project must proceed only on the basis of a 'standard' participant consent, or the new 'broad' consent as discussed above), and must determine whether or not the research project can be conducted using de-identified data instead of personal information.

We submit that s.95 and s.95A should be repealed, and replaced with a single exemption (applicable to APPs 3, 6 *and 8*), the scope of which includes (as relevant and necessary to each project) the collection, use or disclosure of any types of personal information (not just health information), for research projects *in the public interest* (not just medical research), but also including activities preliminary or ancillary to the actual research (such as participant identification and recruitment, and the process of applying de-identification techniques to the data), and the establishment of an enduring asset which will in turn support multiple research projects (e.g. a biobank or significant data asset).

Chapter 16: children

Proposals 16.1 – 16.5 are to:

- Define a child in the Privacy Act;
- Codify that consent must be given with capacity and require entities to decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis, or if that is not practical, assume a child over the age of 15 has capacity;
- Require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child;
- Require entities to have regard to the best interests of the child as part of the 'fair and reasonable' test; and
- Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'.

We are broadly supportive of proposals 16.1 – 16.4 provided they do not rely on, or lead to the introduction of, age verification.

We have concerns regarding proposal 16.5 and its consideration of a risk-based approach to recognising the age of individual users, which may include establishing "age with a level of certainty that is appropriate to the risks to the rights and freedoms of children", indicating that this may be a stalking horse for online age verification.[74] We strongly oppose any proposal that leads to the introduction of age verification, which inherently requires the collection of verified personal information from all users, leading to worse privacy outcomes for everyone. The mechanism by which age is verified is also problematic, for example the collection of government ID or cross-referencing other databases. We further submit that the proposed risk-based approach is not clear and will lead to inconsistent interpretation and application, including the unintended consequence of websites using this as an opportunity to collect more personal information from all users under the guise of confirming that the user is not a child.

We foresee that implementing such a Code will create further compliance burdens for entities as they are forced to establish two sets of operations – one for children and one for adults – and a mechanism to classify and direct users into the correct settings, which again will likely lead to age verification.

While we are supportive of the objective of enabling the robust privacy protection of children, we do not support this proposal.

[74] Privacy Act Review Report 2022, p. 155.

Chapter 18: rights of the individual

We welcome the introduction of new rights for individuals and broadly support the proposals, subject to some minor suggested improvements.

Access and explanation

We support proposal 18.1, however, we submit that proposal 18.1(e) requires some further clarity on what a 'product' is that can attract a nominal fee. Without further clarity, we are concerned the proposal may have unintended consequences in relation to requiring individuals to self-declare vulnerability to have fees waived.

We submit that cost should not be a barrier to individuals exercising their privacy rights and the current proposed phrasing does not impose enough limitation on when a nominal fee can be charged. As the proposal states that fees should be waived for individuals experiencing vulnerability, we are concerned that this may result in the excessive collection of personal information in circumstances where the collection could be avoided by not charging a fee.

We suggest that 18.1(e) should be rephrased to state that unless an entity has incurred actual expenses over and above the reasonable processes that APP 1.2 would require them to implement to comply with this obligation, no fee should be charged.

Objection, erasure, correction, de-indexing

We support proposals 18.2 – 18.5 without amendment.

Exceptions

We support proposal 18.6, but suggest two modifications.

The first is that the Report's position that "[r]ights should always continue to operate to the extent the balancing does not weigh against it"[75] should be explicitly included in any test that entities are required to undertake in balancing exceptions against individual rights. Having a stated position that individual rights should prima facie operate will help ensure entities don't skew the balance towards their own interests.

[75] Privacy Act Review Report 2022, p. 180.

Secondly, we submit that proposal 18.6(c) should be further clarified to ensure entities don't use poor process or system design to excuse not responding to individual requests. For example, where a system does not allow for the deletion of superfluous personal information, entities should be required to take reasonable steps to address the root cause of the issue, rather than merely rely on the technical exception to fulfilling an individual's request.

Response

We support proposals 18.7, 18.8 and 18.10 without amendment. However, we have concerns that the wording of proposal 18.9 establishes an additional exception to the rights of individuals, that being 'it is reasonable to take no steps to comply with the request'.[76] We suggest that the new individual rights adopt the approach formulated in APP 12, which requires the fulfilment of an access request unless an exception applies. Including a 'reasonable steps' test in response to individual rights risks watering down those rights as APP entities are able to determine their own level of compliance based on internal factors and determinations. For example, based on the proposed criteria, it could be open to an APP entity not to comply with a request for access and explanation because they do not perceive themselves to hold high volumes of personal information, there are limited consequences to the individual if the request is not fulfilled, and fulfilling the request would require them to divert resources from other work.

To avoid entities using the 'reasonable steps' test to avoid or undermine the requirement to comply with these new individual rights, we propose that entities' compliance should not be based on a 'reasonable steps' test.

[76] For example, APP 13, another privacy principle related to individual rights, currently stipulates 'the entity must take such steps (if any) as are reasonable in the circumstances'

Chapter 19: automated decision making

Proposals 19.1 – 19.3 are to:

- Require privacy policies to set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect;
- Include high-level indicators of the types of decisions with a legal or similarly significant effect in the Act, supplemented by OAIC guidance; and
- Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

We welcome the addition of proposal 19.3 to the Report. A requirement for entities to provide, on request, information 'more tailored to the specific individual and include an explanation of how a decision was reached'[77] will bring Australia's privacy laws into closer alignment with international standards[78] and community expectations, as described in the Report.[79]

While we support the proposed changes to the Act, we submit that to be truly effective, transparency must offer the ability for individuals to make meaningful choices about the use of their personal information. A right to transparency alone does not necessarily protect privacy, or prevent harm (for example from bias, or disadvantage caused by being in a unique position not contemplated in a model's training data).

The introduction of further rights would go further to bring Australia into line with international standards[80] and the recommendation of the European Commission (noting again, this body will be responsible for determining Australia's adequacy status under the GDPR) that individuals be able to challenge substantially automated decisions with legal or similarly significant effect and obtain a review by a human being.[81]

To that end, we re-iterate our position in our submission to the Discussion Paper[82] and call again for the introduction of a right to obtain a human review of a decision made by automated means.

[77] Privacy Act Review Report 2022, p. 192.
[78] For example, GDPR Article 13
[79] Privacy Act Review Report 2022, p. 192.
[80] For example, GDPR Article 22.
[81] European Commission, 'Consultation on the review of the Privacy Act 1988' p. 4.
[82] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, p. 40.

Chapter 20: direct marketing, targeting and trading

We recognise and support the intention to create additional protections for individuals when it comes to potentially harmful practices associated with targeting systems and the trading of personal information.

However, while we recognise the intention behind these proposals, we are concerned that in practice they will undermine the technological neutrality and principles-basis of the Act, lead to further confusion, and encourage bad actors to structure practices in such a way so as to avoid capture by the proposed provisions. We are further concerned that too many concessions have been made for the privacy-invasive practices that support the business models of ad-supported platforms, which treat individuals' data as an asset they can use commercially, in essence legitimising the very activities that these reforms set out to tackle.

We recognise that many businesses carry out legitimate marketing activities well within the expectations of the community, and often to the benefit of their customers and prospects. We submit that the reforms proposed in this Report should enable, rather than hinder, direct marketing activities undertaken by entities which do not rely on targeting systems or data brokerage businesses, and satisfy the requirements of the fair and reasonable test. This will ensure that businesses have an effective channel via which to conduct reasonably expected marketing activities without needing to resort to more invasive ways of identifying and targeting audiences.

We submit that adopting a more principles-based approach, as advocated for in our discussion on Chapter 4, will not only preserve the principles-basis and technological neutrality of the Act, but lead to better privacy outcomes for individuals.

Definitions

Proposal 20.1 is to include definitions in the Act for 'direct marketing', 'targeting', and 'trading'. We support the intention to create more clarity and address definitional challenges within the Act, however, we submit that these definitions require modification in order to achieve these goals without leading to further confusion.

Direct marketing

We submit that the definition of 'direct marketing' should be amended to clarify that direct marketing activity based on personal information will become 'targeting' where that personal information is shared with an entity that is not prohibited from collecting and using that

personal information for its own purposes. So, for example, where a service provider is contractually engaged, with appropriate data use limitation clauses, to distribute marketing material on behalf of the APP entity, this would fall within the definition of 'direct marketing'. However, where a mailing list is uploaded to Facebook, which would be able to collect and use that information for its own purposes in addition to those of the entity conducting the marketing activity, this should be an example of 'targeting'.

Targeting

We submit that the definition of 'targeting' in its current form will lead to increased confusion, particularly due to its reliance on the terms 'deidentified' and 'unidentified' information, and will become quickly outdated.

This definition of targeting would be much clearer if the definition of 'personal information' first included information where an individual may be singled out and acted upon, even if their identity is not known (see discussion above in relation to proposal 4.4), because then targeting would not need to rely on bringing in 'de-identified' and 'unidentified' information into its definition. In our experience, clients prefer to have clarity rather than so much flexibility that it, in practice, increases their compliance burden as they try to determine or interpret their obligations. We submit that requiring entities to navigate between personal information, de-identified information and unidentified information just to determine whether information falls within the scope of this very specific practice is an undue compliance burden which could be alleviated with a more principles-based definition of 'personal information'.

Aside from the compliance burden, we foresee this definition leading to arguments over the 'which relates to an individual' component of the definition, as companies structure 'de-identified' or 'unidentified' data practices to fall into grey areas outside of this definition (e.g. segregating data so that unidentified elements relate to a device ID, using 'clean rooms' to segregate the purposes for which data is processed). The risk of focusing the current definition on existing practices is that practices can easily evolve to avoid the definition, leading to a quickly outdated definition, and thus obsolete regulations.

Again, our concerns are not merely theoretical. When the introduction of the GDPR threatened Meta's behavioural advertising business model in the EU, particularly when determining a lawful basis for processing to rely on for these practices, the recent EDPB Binding Decisions illustrate that Meta structured what was argued to be forced consent to look like a contract.[83] We foresee that when definitions allow for so much confusion and cross-referencing of other definitions, similar arguments will arise in Australia (i.e. that a particular practice was not 'targeting' for the purposes of the definition in the Act).

[83] European Data Protection Board, 'Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)', Adopted on 5 December 2022; European Data Protection Board, 'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)', Adopted on 5 December 2022.

Thus we submit that, as per our discussion on Chapter 4 (including the risks of basing definitions on the claimed purpose of the activity), the definition of 'personal information' must first be changed to include information where an individual may be singled out and acted upon, even if their identity is not known. The definition of 'targeting' can then be 'capture the collection, use or disclosure of personal information for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class)'. The alteration of the definition of 'personal information' would also mean that any practices that do not fall within the definition of 'targeting' would still be captured by the fair and reasonable test and the requirements of APP 6, thus leading to robust protections for individuals with less room for the exploitation of loopholes in definitions.

Trading

We submit that the definition of trading is too narrow and should cover the collection of personal information, as well as its use and disclosure.

Individual rights on direct marketing, targeting and trading

Proposals 20.2 – 20.4 are to:

- Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes;
- Provide individuals with an unqualified right to opt-out of receiving targeted advertising; and
- Introduce a requirement that an individual's consent must be obtained to trade their personal information.

Direct marketing

We are supportive of proposal 20.2, however, submit that the right should be further clarified to explicitly state that if individuals opt out of direct marketing, this would extend to any use of their data for processes that underpin the direct marketing (for example, profiling, segmenting, audience creation). If this point is not clearly explained, we foresee it leading to the inconsistent application of this proposal, and a failure to fully implement individuals' wishes.

We submit that the direct marketing proposals could be further strengthened by specifying in the Act that direct marketing will only be 'fair and reasonable' if the personal information was collected directly from the individual (who must have been an adult at the time of

collection), in circumstances where direct marketing is a directly related secondary purpose to the original purpose of collection, and if the individual was given notice of the collection and proposed use for marketing, and they were given the option to 'opt out', and the individual has not opted out.

Targeting

We are deeply concerned about the limitations on individual rights in proposal 20.3. While the right to opt-out has been framed as 'unqualified', it is in fact subject to significant qualifications (i.e. that entities can continue to use individuals' data for targeting purposes), leading to ongoing privacy harms for individuals which the Report itself had articulated.[84] We respectfully submit that allowing the continued use of personal information (de-identified, unidentified or otherwise) despite an individual's wishes to opt out will not at all address the harms described in this Report and only further entrenches power imbalances between individuals and entities who operate targeting systems. The proposal also shifts the compliance burden from entities to individuals, who would need to navigate multiple websites to exercise very limited rights, and risks being misleading to individuals who believe they have exercised an unqualified opt-out right, only to find that, while they no longer see ads, their personal information is still being used and disclosed to facilitate targeting systems.

We submit that proposal 20.3 is not in line with community expectations. In its 'Not a fair trade' Working Paper, the Consumer Policy Research Centre found that only 9% of Australians reported being comfortable with companies targeting them with advertising based on their online behaviour where they had not consented to targeting.[85] Additionally, in its 2021 Future of Marketing Research report, Adobe found that the top three brand behaviours that consumers regard as trust-breaking are: 1) creepiness — i.e. online tracking and sending marketing emails without permission or when consumers don't expect the ad or don't remember giving their data; 2) annoyance — sending too many emails or texts, not being clear about privacy policies or what brands do with consumer data; and 3) not listening — when brands continue to send comms or bombard with ads, even after consumers have opted out.[86]

Instead of proposal 20.3, we again call for a principles-based approach. If the definition of personal information was to include information where an individual may be singled out and acted upon, even if their identity is not known, this would create proactive obligations on entities, rather than leaving individuals to navigate multiple websites to exercise very limited rights. APP 6 should then be amended to specify that targeting can never be considered a primary purpose or 'related' secondary purpose. Therefore, organisations will need individuals to 'opt in' via consent to target the individual, unless another law allows it.

[84] Privacy Act Review Report 2022, pp 199-201.
[85] Consumer Policy Research Centre 'Not a fair trade: Consumer views on how businesses use their data' 12. Available at https://cprc.org.au/wp-content/uploads/2023/03/CPRC-working-paper-Not-a-fair-trade-March-2025.pdf
[86] https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk

Entities must have a proactive obligation on them to deal with the personal information they hold (including that held for the purposes of targeting) in compliance with the APPs. We submit that this can only be achieved by adopting a more principles-based approach.

Finally, we continue to be concerned about the likely use of 'dark patterns' in these scenarios to make it increasingly difficult for individuals to exercise their rights. As previously discussed, it is concerning that years after the implementation of the GDPR and ePrivacy Directive, Supervisory Authorities and the EDPB are still required to address issues of 'dark patterns' in cookies banners. We are not alone in our concerns; law academic Katharine Kemp recently expressed her concerns regarding the use of 'dark patterns' in response to this proposal: "Although having the option to opt out of seeing targeted ads gives consumers some limited control, companies still control the 'choice architecture' of such settings. They can use their control to make opting out confusing and difficult for users, by forcing them to navigate through multiple pages or websites with obscurely labelled settings."[87] Non-binding OAIC guidance will not prevent 'dark patterns', however, ensuring entities have proactive obligations on themselves to comply with the APPs will go a long way to ensuring individuals' data is handled appropriately in the first place, without them needing to exercise specific rights.

Trading

We refer back to the significant concerns set out in our discussion at Chapter 11 on consent in relation to proposal 20.4 and submit that the privacy harms associated with trading should be addressed in a principles-based approach, rather than the current proposal in the Report. Consent for trading should not be permitted to be tied to terms of service.

We submit that instead of proposal 20.4, APP 6 should specify that trade in personal information cannot be considered a primary purpose or directly related secondary purpose, which means it will only be lawful with consent or under a public interest exemption. This will remove the need to create separate provisions on consent for trading, which we continue to be concerned about, as outlined above in relation to the discussion of consent.

Consent fatigue

We recognise the Report's position on ensuring that any proposals do not result in consent fatigue for individuals. However, we submit that current perceptions on the nature of consent in an online environment are largely driven by the use of 'dark patterns' to deliberately steer individuals into selecting the privacy setting that is in the interests of the entity. As part of a series of complaints raised against non-compliant cookie banners by privacy advocacy group NOYB, Max Schrems recently stated "[a] whole industry of consultants and designers develop crazy click labyrinths to ensure imaginary consent rates. Frustrating people into clicking 'okay' is a clear violation of the GDPR's principles. Under the

[87] https://theconversation.com/proposed-privacy-reforms-could-help-australia-play-catch-up-with-other-nations-but-they-fail-to-tackle-targeted-ads-200166

law, companies must facilitate users to express their choice and design systems fairly. Companies openly admit that only 3% of all users actually want to accept cookies, but more than 90% can be nudged into clicking the 'agree' button".[88]

Australia has the benefit of leveraging lessons learnt from the EU in the design of online consent options, including recent advice on common 'dark patterns' issued by the EDPB's 'cookie banner taskforce',[89] to ensure consent requests are fair to individuals. We submit that choice architecture decisions specifically designed to frustrate users into giving their consent should not be conflated with the overall principle of seeking opt-in consent and the benefits this will offer individuals. We submit that if reforms call for pro-privacy settings in consent banners, consent fatigue can be avoided.

Children

We welcome **proposals 20.5 – 20.7** to:

- Prohibit direct marketing to children unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests;
- Prohibit targeting to children, with an exception for targeting that is in the child's best interests;
- Prohibit trading in the personal information of children.

We submit that proposal 20.6 should specify that the child must have opted in to targeting and that targeting is not based on any sensitive information.

In implementing these proposals, we suggest that the Bill be drafted to reflect the principles-basis of the Act. This could occur by incorporating these requirements in the fair and reasonable test or modifying existing APPs.

Accountability for targeting

Proposals 20.8 and 20.9 are to:

- Require targeting to be fair and reasonable in the circumstances;
- Prohibit targeting based on certain sensitive information, with an exception for socially beneficial content; and
- Require entities to provide information about targeting.

[88] https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints
[89] See https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

For reasons already discussed, we submit that proposal 20.8(a) does not go far enough in protecting individuals – targeting should be subject to all APPs, not just the proposed carve outs in the Act.

We are concerned that proposal 20.8(b) will result in leaking sensitive information into the Adtech and data brokerage ecosystem since the publishers of socially beneficial content must rely on these systems in order to target individuals. This will result in Adtech companies being able to collect that sensitive information to use for their own purposes. As such, we submit that there should be a prohibition on the use of *any* sensitive information for the purposes of targeting.

We have no objections to proposal 20.9.

Chapter 22: Controllers and processors of personal information

We oppose proposal 22.1 as it will add significant complexity and confusion to the Act, without delivering tangible benefits. We echo concerns raised by various submissions (as discussed in the Report) which highlighted the increased compliance burden, with minimal benefit for consumer privacy rights.[90]

We believe having a single set of obligations for all entities is a far clearer approach in the Australian context. We foresee the introduction of controllers and processors merely leading to arguments over which role each entity plays, particularly in the instance of joint controllers and sub-contracting arrangements.

We submit that a faster removal of the small business exemption will lead to far better outcomes for businesses and consumers alike.

[90] Privacy Act Review Report 2022, pp 231.

Chapter 26: direct right of action

We support a direct right of action. However, we submit that the current proposal, namely the requirement to exercise this right via the Federal Court, will make this inaccessible for the vast majority of individuals.

We re-iterate the points made in our submission to the Discussion Paper[91] and submit that in order to have ready access to justice, an alternative avenue to the Federal Court must be introduced.

[91] Salinger Privacy Submission to the Privacy Act Review Discussion Paper, pp. 44-45.

About the authors

This submission was prepared by Anna Johnston and Alex Kotova.

Anna Johnston is founder and Principal of Salinger Privacy. Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

In 2022, Anna was honoured for her 'exceptional leadership, knowledge and creativity in privacy' with the IAPP Vanguard Award, one of five privacy professionals recognised globally whose pioneering work is helping to shape the future of privacy and data protection. While her day-to-day work involves assisting clients to develop innovative approaches to privacy protection, the Vanguard award was bestowed in reflection of Anna's contributions to the privacy profession, and to the protection of privacy for the benefit of all.

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

Alex Kotova, our Privacy & Technology Specialist, has developed her privacy expertise through roles across multiple industries, including banking, retail, hospitality, gaming and health insurance.

Alex has particular expertise in applying privacy principles to the rapidly moving technology landscape, including the implementation, use and governance of expert systems (including artificial intelligence, machine learning, and algorithms) and other emerging technologies. She has advised extensively on third-party software, complex data flows, and data sharing arrangements. She has a special interest in the operation of data ecosystems, including AdTech and data brokerage.

Alex holds a Bachelor of Laws / Bachelor of Arts, a Graduate Diploma of Legal Practice and was admitted as an Australian Lawyer in Victoria in 2015. She is also a member of the IAPP, a Certified Information Privacy Manager (CIPM), and Certified Information Privacy Professional – Europe (CIPP/E).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

SalingerPrivacy

We know privacy inside and out.

Salinger Consulting Pty Ltd

ABN 84 110 386 537

PO Box 1250, Manly NSW 1655

www.salingerprivacy.com.au