10 January 2022

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*

Please find attached a joint submission of IIS Partners and Ground Up Consulting in response to the **Privacy Act Review – Discussion Paper (October 2021)**.

We make this submission as specialist privacy and security practitioners with deep experience in privacy impact assessment; privacy by design; privacy program development, management and acculturation; strategic privacy risk management; data breach response; and disciplinary and practical linkages to information security.

We have no objection to publication of our submission and no redactions of personal information herein are required.

Thank you for the opportunity to provide comment on this important area of law and practice. Please contact either of the undersigned authors if you require clarification on any aspect of this submission.

Michael S. Trovato

Managing Director, IIS Partners

Malcolm Crompton AM

Founder and Lead Privacy Advisor,

IIS Partners

Nicole Stephensen

Director and Principal, Ground Up Consulting

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

GROUND UP
Consulting

Table of Contents

Introduction

In the context of Australian privacy law reform, setting expectations is vital. 'Privacy' in our region (as in, our rights and freedoms broadly in respect of privacy) is a concept applied through a narrower lens of 'information privacy' (that is, privacy in relation to information about a person).

It is through privacy law, and associated education, awareness and outreach of the privacy regulator, that we shape the expectations of the community about what government and organisations may do with their personal information. This is an enormous responsibility, particularly in light of the burgeoning digital economy; increasing availability and sophistication of technologies and the preoccupation with data across all sectors – from government service delivery, to adtech, to social media, to e-commerce, to banking, to healthcare; and the cyber threats from nation and non-nation states and organised crime – where the notion of 'privacy' has implications for the community beyond the narrow frame of reference ascribed to 'information privacy'.

Privacy law is intended to be both instructive to good decision-making in respect of collection and handling of personal information and responsive to community expectations in this regard. On the latter, it is vital that Australian privacy law reform preserves what is intended to be a beneficial scheme for the community we serve, where the ability of the government and organisations to collect and handle personal information for their purposes is interpreted **narrowly** (and with utmost clarity) and the rights of individuals in respect of what happens to their personal information are interpreted **broadly** (and to the greatest benefit of the community).

We support the general trajectory of the Discussion Paper and consider that many of the proposals therein would sustain the intention of privacy law as a beneficial scheme. We also acknowledge the submissions of the Office of the Information Commissioner (OAIC) and Salinger Privacy as providing comprehensive feedback on the Discussion Paper in its entirety with which our position is aligned.

Key Considerations

We have chosen to respond to selected questions posed by the Discussion Paper, to detail our views on specific matters raised and key considerations from our perspective as experts in the field:

- Defining personal information;
- Application of the Act – in particular, removal of the small business exemption;
- Consent; and
- Adequate resourcing of the OAIC.

The remainder of our submission deals with these four items in turn and we highlight in each case our **recommendation**.

Defining Personal Information

Our understanding of proposals 2.1 - 2.3 in the Discussion Paper is that the proposed new definition of personal information will be:

> *Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:*
>
> *a) whether the information or opinion is true or not; and*
> *b) whether the information or opinion is recorded in a material form or not.*
>
> *An individual is 'reasonably identifiable' if they are capable of being identified, directly or indirectly.*

Is 'reasonably' a necessary condition for identifiability?

It is our view that the word 'reasonably' attached to 'identifiable' in the definition of personal information may be problematic in its application. What is reasonable in the ordinary course of work based on existing business resources – including technological acumen or sophistication, or lack thereof – will vary across activities and sectors and is likely to be subject to generous interpretation (in favour of the government and organisations) when making decisions about what is, or is not, personal information in their particular contexts.

The word 'reasonably' in this context is a hangover from the existing definition of personal information and associated regulatory guidance. For instance, the OAIC said in its 2018 report on the Department of Health's publication of MBS/ PBS data that *"[w]hether an individual is reasonably identifiable depends on the nature of the information in issue, and the context in which the information is held or released"* and, further, that an individual will be reasonably identifiable *"where the process or steps for that individual to be identifiable are reasonable to achieve"*.[1]

[1] https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/mbspbs-data-publication

It was the OAIC's view that the techniques applied to re-identify MBS/ PBS recipients in that case were not reasonably (i.e., easily) achieved by ordinary persons; however we submit that the very ability to do so (which was easily done by the data experts in the ordinary course of their work) suggests broad ranging sophistication in respect of entities handling personal information – and this sophistication will only improve with technological advances and data-driven career specialisations across sectors.

Further, we submit that the presence of identifiability alone is enough to render information personal – which is echoed by privacy jurisdictions globally, many of which have recently modernised or created new privacy laws that exclude the word 'reasonably' altogether as part of the test for identifiability.

We **recommend** removing the word 'reasonably' from 'reasonably identifiable' in the proposed new definition of personal information.

Being clear about individuation for tracking, tracing, monitoring, and targeting of individuals

Even in the guise of service provision, offering benefits or aligning with an individual or cohort's preferences, there is a creepiness to privacy practice in some sectors that is perpetuated by various interpretations of the definition of personal information. The Privacy Commissioner v Telstra decision heralded this modern problem years ago when it excluded location data from being 'personal' in the circumstance and turned years of privacy leadership and 'what is personal information' acculturation on its head.[2]

In the current digital economy, which is fuelled largely by data, the question of what personal information is – and, in particular, when a person is 'identifiable' – is vital to address with clarity and limited room for interpretation.

Information about a person these days need not identify them; rather, it may be their cumulative digital exhaust vulnerable to exploitation by data brokers or cybercriminals, or information that is ostensibly 'de-identified' yet still allows a person to be tracked, traced, or targeted even if they are not knowable. This notion of individuation (but not identification) is discussed at length in a 2020 Brussels Privacy Hub Working Paper that queried whether our definition of personal information remains fit for purpose,[3] and is further illustrated by the complex digital twins that can be compiled of an unknown (i.e., not identified) person within a cohort, which is the purview of companies like LiveRamp (formerly Acxiom).[4]

---

2 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4. OAIC summary of the decision: https://www.oaic.gov.au/updates/news-and-media/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision

3 https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL6-N24.pdf

4 https://liveramp.com

Victorian Information Commissioner, Sven Blummel, summed up this modern privacy challenge perfectly in a recent privacy network meeting:

> *"I can exploit you if I know your fears, your likely political leanings, your cohort. I don't need to know exactly who you are; I just need to know that you have a group of attributes that is particularly receptive to whatever I'm selling or whatever outrage I want to foment amongst people."*[5]

Page 27 of the Discussion Paper states that a new definition of personal information "would cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named". We consider this to be a meaningful and welcome development.

We **recommend** the new definition of personal information must include a definition of the word 'identifiable', and further, that drafting notes include a test relating to the ability to discern or recognize one individual as distinct from others (whether or not a person is ultimately knowable).

To this end, we support the drafting suggestions made by Salinger Privacy in their 03.1.2022 submission on the Discussion Paper, which would see the definition of personal information include a definition of 'identifiable' as follows:

> *"(i) able to be identified directly or indirectly, or*
>
> *(ii) able to be discerned or recognised as an individual distinct from others,*
>
> *regardless of whether their identity can be ascertained or verified".*

And, further, the inclusion of a clarifying drafting note as proposed by Salinger for 'able to be discerned or recognised as an individual distinct from others', as meaning:

> *"if the individual, or a device linked to the individual, could (whether online or offline)*
>
> *be:*
>
> (i) *surveilled, tracked, located or monitored; or*
>
> (ii) *profiled, contacted, or targeted in order to be subjected to differential treatment in the form of any action, decision or intervention including the provision or withholding of information, content, advertisements or offers; or*
>
> (iii) *linked to other data which relates to the individual".*

[5] Sven Blummel, virtual Victorian Privacy Network Meeting, 11 Nov 2021. Video recording: https://vimeo.com/644635219

Application of the Act – Exemptions

There are a number of current exemptions from application of the Privacy Act canvassed in the Discussion Paper, including:

- Small business;
- Employee records;
- Political acts and practices; and
- Journalism.

We strongly support removal of all four of the exemptions. Indeed, reflecting on comments made by one of our authors during his time as Privacy Commissioner of Australia, meaningful attention to the exemptions from the perspective of the community is long overdue:

> *"If we are to have a community that fully respects the principles of privacy and the political institutions that support them, then these institutions themselves must adopt the principles and practices they seek to require of others. I believe that political organisations should follow the same practices and principles that are required in the wider community."* [6] – Malcolm Crompton, former Federal Privacy Commissioner

In this submission, we focus on the small business exemption.

Notes on the Small Business Exemption

Among our clients, the question of the small business exemption is divisive. Some small businesses – in particular, those with close ties to the community – are open to opting-in to the Australian Privacy Principles (APPs) to demonstrate accountability and trustworthiness in their information practices. Others are quite happy to gather, use, share and even sell personal information just because they can.

The current pandemic has seen the 'pivoting' of many small businesses to previously underutilised online environments, as well as the leveraging of the COVID-19 crisis by start-ups to create new apps and services that involve the ingestion of personal information, which has served to highlight a significant gap between what the law requires and what the community expects.

[6] Media Release dated 12.4.2000: https://webarchive.nla.gov.au/awa/20040915164537/http://pandora.nla.gov.au/pan/21204/20010814-0000/www.privacy.gov.au/news/00_05.html

Retaining the small business exemption means that small businesses - including start-ups and microbusinesses – will avoid the accountability, responsibility, expense, and compliance challenges of managing personal information in accordance with the APPs (arguably challenging for even well-resourced larger organisations). However, retaining the exemption perpetuates (and potentially exacerbates) a gap in information practice at the small business level, which may no longer be acceptable to the community when considered in the contexts of technology proliferation and the increased use of personal information by businesses for online sales and marketing, background analytics and data-related partnerships (e.g., the use of social media to engage with, and sell to, clientele).

We **recommend** the removal of the small business exemption, with the caveats that the OAIC is adequately resourced to address anticipated advisory and complaints management burden and that there is an adequate grace period provided to small businesses to ensure they are compliance-ready.

Prohibitive cost of an External Dispute Resolution (EDR) scheme for small business (24.9)

If the small business exemption is removed, small businesses will become APP entities for the purposes of the Privacy Act. This attracts questions in relation to enforcement, and the proposals noted in 24.9 of the Discussion Paper with respect to alternative regulatory models. We note that many small businesses are microbusinesses (1-5 staff), including some start-ups exploring the efficacy of a product or service offering. Others operate on a limited budget.

We submit that the notions of wrapping small businesses in an EDR scheme (Option 1) or a fee-paid scheme (Option 2) should be expected to be unpalatable to small businesses and outside of their reasonable expectations of being brought into the fold of Australia's privacy regime. We **recommend** expanding the capacity of the OAIC (Option 3), which (certainly from a community perspective) appears to be less complex and far more intuitive.

Interaction with state/ territory regulators - small business commissioners (28.2)

Many small businesses have practical and meaningful ties to the Small Business Commissioners in their states and territories.[7] It is unlikely to be a reasonable extension of the role of those Commissioners to localise enforcement of federal privacy rules; however, to limit advisory burden on the OAIC, there may be opportunity to enter into advisory agreements whereby a state or territory Small Business Commissioner is empowered to advise small businesses within their jurisdiction about best privacy practice, application of the APPs, information security considerations and so forth.

[7] Queensland's Office of the Small Business Commissioner has, on the basis of an influx of questions from the Queensland business community, recently issued advice (inclusive of privacy) to small businesses on considerations

We submit, however, that all efforts should be taken to avoid confusion within the small business community and that seeking practical support from Small Business Commissioners (or other entities outside the OAIC, such as state/ territory Privacy Commissioners) may unnecessarily complicate the pathways through which small businesses can seek support and advice.

Consent (9.1)

We support the direction of the Discussion Paper (and the OAIC's submission in this regard) towards increased organisational accountability and responsibility through stronger consent provisions. This, we hope, will have the effect of making fair the seemingly *de facto* approach to business – and personal information handling – that currently places responsibility of managing privacy outcomes squarely on the shoulders of the individual.

We **recommend** the proposal at 9.1 in relation to defining consent as voluntary, informed, current, specific and unambiguous; however, it remains unclear why the proposed OP Code (under the Online Privacy Bill) should also stipulate consent requirements when amendments to the Privacy Act could comfortably address the same matters and extend to all APP entities operating in both digital and analogue environments. Indeed, and as an aside, we do not support the introduction of yet another layer of complexity to privacy in Australia through the OP Bill and the consequential OP Code when thoughtful amendments to the Privacy Act to account for online environments would have the same effect and – likely – more gravitas.

Conflating transparency mechanisms with 'getting consent' (8.1 - 8.4 and 9.1 – 9.2)

Online platforms and services are increasingly conflating transparency efforts with a person's active consent to collect, use and disclose all manner of their personal information in all manner of ways.

In government contexts, in particular those associated with the provision of services or benefits to the community, we regularly see collection notices bundled with consent, usually by way of the collection notice containing a tick box indicating that "*Having read this notice, I agree to the use of my personal information for this service/ program/ initiative*". We **recommend** clarity, whether via explanatory notes or targeted OAIC advice, that giving notice is not the same as asking for permission and that the two process are, in fact, distinct.

pertaining to COVID-19 vaccination status - https://www.publications.qld.gov.au/ckan-publications-attachments-prod/resources/5cfb05ee-f5ff-495d-a88e-96f88cfbf114/qsbc_key-covid-links-for-qld-small-business-v5.pdf?ETag=%224215d35ab72f3fb7a6266c805b5f89cf%22

The privacy profession utters a collective groan each time we read, "*By continuing to use this site, you consent to our Privacy Policy*". As with notice, a privacy policy informs… it does not ask. Reading and understanding a privacy policy is not an appropriate vehicle for gathering consent – it is a transparency mechanism that informs a person; however, it fails to demonstrate the voluntariness, currency, specificity or lack of ambiguity aspects of the 'VICSU' test. Simply telling a person what is intended with their personal information 'generally' is not the same as drawing parameters around a specific use or disclosure of personal information, setting a timeframe for which the consent is valid, ensuring a person feels empowered not to consent or asking them if – in this case – an activity involving their personal information is okay with them, if they agree, if they are happy to proceed. We **recommend** that law, or the explanatory notes, should explicitly state that a person 'having read the privacy policy' does not meet the test for consent as suggested by the reforms.

The illusion of 'choice and control'

An intention of privacy law is to place specific limits on what happens to personal information through its lifecycle – from the moment it is collected (and even before that in terms of good decision-making) through to its destruction. Relevant to achieving this intention are requirements around honouring the purpose of collecting personal information; limiting its use; and limiting when it can be shared or otherwise disclosed.

A vast proportion of government and private sector organisations are, at present, comfortably (and erroneously) requiring individuals to 'consent away' all the intended restrictions of the Privacy Act. They do this by 1) conflating transparency efforts with consent (as discussed above) and 2) by defaulting to broad-brush consent (usually in the context of a 'contract of service') as the easiest means to achieve a desired end. The sign-up processes for online accounts – ABC iView, for example – is a good illustration.[8]

While we support the proposal at 9.1, we caution that consent – and its application in a business context – must remain the 'exception' to limitations on use and disclosure of personal information set out in the APPs and should not be considered 'the rule'. That is, we **recommend** it must not become the default catch-all alternative to good privacy practice. Use consent as an available mechanism to permit use and disclosure of personal information only when the other exceptions have first been exhausted.

[8] https://iviewsupport.abc.net.au/hc/en-us/articles/360003865776-How-do-I-sign-up-for-an-ABC-Account-

Adequate resourcing of the OAIC

A chief criticism of privacy law establishment and reform in Australia to date is the critical underfunding of the regulator. That the OAIC is weak and dysfunctional because of under-resourcing has been raised in a bulk of submissions from civil society representatives and privacy experts (and even commiserating privacy regulators from other states!) in relation to privacy law reform in Australia for decades. It is also a hot topic in the media.

If the Privacy Act is ever to regulate the personal information collection and handling practices of government and organisations – inclusive of education and advisory services, undertaking investigations, managing enquiries and complaints from the community, and taking legal action – a shoestring budget and chronic understaffing of key roles will not suffice. It will, if the current trend continues, serve only to embarrass the government and leave egg on the face of a deeply committed regulator who is tasked with myriad functions.

We strongly **recommend** adequate resourcing of the OAIC across advisory, intake, complaints management, investigation, and other functions to achieve any meaningful uplift to – and longevity of – Australia's privacy regime.

We submit that privacy law reform as canvassed by this Discussion Paper must be budgeted for at the outset and not relegated to 'within existing capacity of the OAIC'. A failure to do this may result in 'on paper' reforms that are without teeth, thereby diminishing community trust in the efficacy of the OAIC, and the Privacy Act itself, and allowing organisations to 'risk manage' their personal information handling practices with impunity.

Conclusion

We thank the Attorney-General for including us in the consultation process and the opportunity to contribute to this phase of privacy law reform in Australia. We would be pleased to discuss any aspect of our submission or any other issues.

If you have any questions or need additional information, please do not hesitate to contact us (details overleaf).

Authors

Michael S. Trovato, GAICD, MAISA, CISM, CDSPE, CISA

Managing Director and Lead Security Advisor, IIS Partners

mtrovato@iispartners.com | +61 404 880 793

Nicole Stephensen, FAISA, SCCISP

Director and Principal, Ground Up Consulting

nicole@groundupprivacy.com.au | +61 433 688 118

Malcolm Crompton AM, FAICD, CIPP

Founder and Lead Privacy Advisor, IIS Partners

mcrompton@iispartners.com | +61 407 014 450

Research

Sarah Bakar

Consultant, IIS Partners

sbakar@iispartners.com

Information Integrity Solutions Pty Ltd

PO Box 978, Strawberry Hills NSW 2012, Australia

iispartners.com

Ground Up Consulting Pty Ltd

3/ 20 Gray Street, Ipswich QLD 4305, Australia

groundupprivacy.com.au