29 March 2023

Attorney-General's Department
4 National Circuit
BARTON ACT 2600
privacyactreview@ag.gov.au

Dear Attorney-General,

Feedback to inform the Government response to the Privacy Act review

Thank you for the opportunity to offer feedback to inform the Government's response to the Privacy Act review report (the Report).

We make this submission (attached) 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; disciplinary and practical linkages to information security; and contributing extensively to thought leadership on information governance in Australia and internationally.

In this submission, our comments are confined to some key areas of interest which include: the definition of personal information, exemptions, consent, the fair and reasonable test, targeting and regulator resourcing.

We are happy for our feedback to be published in full without redactions. Should you have any questions in relation to the contents of this submission, these may be directed to any of the authors, whose details are provided on the submission's final page.

Yours sincerely

Michael S. Trovato
Managing Partner

Malcolm Crompton AM
Founder and Partner

Nicole Stephensen
Partner

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Submission on the Privacy Act Review Report

Getting the balance right

We commend the reviewers on their Report which addresses a wide range of complex matters with nuance and detail.

Currently the *Privacy Act 1988* is out of balance, placing far too much emphasis on individuals exercising privacy rights (like consent) and far too little focus on ensuring that entities live up to their responsibilities and do the right thing with regard to privacy. Consent mechanisms are buckling under the weight of overuse and have too often been used to override privacy rather than protect it. We therefore agree with the approach the Report has taken to rebalance the Act by limiting further expansion of consent and, instead, compelling fair and respectful data use, including via the proposed introduction of a fair and reasonable test.

Privacy and democracy

In the 21st century, democracies around the world are under pressure from forces enabled by digital technology and the internet. Political polarisation, loss of trust in institutions and experts, 'fake news' and disinformation, the rise of big tech monopolies – all of these find their roots in increasingly sophisticated digital technology and all have implications for democracy.

If we are to safeguard democracy and address those challenges, part of the answer will be fostering trust online and enabling space for individuals to learn, socialise and participate without surveillance and without being unconsciously manipulated by recommender systems driven by algorithms that are ultimately obscure. Strong privacy arrangements are therefore a critical aspect of reigning in the excesses of a digital environment that has allowed, and at times actively encouraged, serious breakdowns in the democratic process.

We therefore encourage the Government to understand these reforms in their wider context: as a necessary intervention to safeguard both individuals and our democracy and give overdue attention to the public interest in privacy.

Definition of personal information

The definition of personal information in the Privacy Act sets the Act's regulatory parameters, since the Act is, in large part, constrained to regulating the collection and handling of personal information. As such, the scope of the definition has enormous implications for the Privacy Act and its effectiveness. Narrowing the definition in any way would risk excluding activities that seriously affect individual privacy.

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

The series 4 proposals outline several reforms to the definition of personal information. Largely, these proposals are 'clarifying amendments' in the sense that they add further certainty to the framing of the definition but do not substantially change the operation of the Act. For that reason, they should be uncontroversial and straightforward to take up.

We **support** the series 4 proposals, particularly proposals 4.1 and 4.6.

Small business exemption

The small business exemption was originally incorporated into the Privacy Act in recognition of the regulatory burden that privacy compliance might impose on businesses with negligible information holdings. However, circumstances have changed and small businesses are now much more likely to have an online presence and to process and store personal information.

In our submission to the Discussion Paper, we recommended the removal of the small business exemption. We therefore **support** proposals 6.1 and 6.2. We agree, in line with proposal 6.1, that small businesses will need support to adjust their privacy practices and comply with the Privacy Act, hence why it is critical that the Office of the Australian Information Commissioner (OAIC) be appropriately resourced to offer that support (see also our comments below on enforcement).

While preparations for proposal 6.1 are underway, we support removing the exemption for small businesses that obtain consent to trade in personal information – per proposal 6.2. This aligns with our concern that the Privacy Act should no longer allow individuals to 'consent away' their privacy rights, particularly in cases such as this one where it may not be clear that giving consent completely removes the protection of the Act.

Employee records exemption

The Report found that there were legitimate concerns about the adequacy of privacy protections for employee records, particularly given the amount and sensitivity of the information in question. In relation to proposal 7.1, we are concerned that differential treatment of employee personal information will lead to needless fragmentation of privacy obligations. A central consideration for the reforms should be reducing complexity where possible.

The exemption should be removed rather than subject to conditions and exceptions. Currently APP entities that are agencies must comply with the APPs in relation to their employee records. It is not clear why extending this coverage to the private sector would raise different or problematic considerations.

Political exemption

Political organisations are exempt from the Privacy Act by virtue of sections 6C and 7C. Exempting political entities from the Act was intended to encourage freedom of political speech. However, as the Report points out, advances in technology which have increased the volume of information about voters that can be collected and harnessed for political influence have raised legitimate concerns about privacy risks.

We **support** removal of the political exemption and therefore support the series 8 proposals. Political organisations should follow the same practices and principles that are required in the wider community. Imposing some of the requirements of the Privacy Act would not stop political parties collecting and using personal information but would apply appropriate guardrails to information handling.

Consent

Worldwide, privacy and data protection laws, including the much-vaunted EU General Data Protection Regulation, have been neutered by consent provisions that provide no limit on that to which the individual can consent. We have observed (particularly in online contexts) the ongoing erroneous use of Terms, 'privacy' notices and policies to which individuals are asked to consent – with these presented on a take it or leave it basis and requiring a person to consent to potentially limitless provisions. The result has been that most individuals around the world who are nominally protected by these laws have consented away any limits on collection, use and sharing of their personal information. Australia is no exception.

As such, the consent provisions are by far the weakest link in privacy frameworks because they effectively remove the protections that the frameworks would otherwise provide. We therefore agree with the approach the Report has taken to rebalance the Privacy Act by limiting further expansion of consent and, instead, compelling fair and respectful data use, including via the proposed introduction of a fair and reasonable test. We would disagree with any move to change or weaken this approach.

We **support** proposals 11.1, 11.2 and 11.3. Largely, these proposals are 'clarifying amendments' in the sense that they add further certainty to the framing of provisions in the Privacy Act but do not substantially change the operation of the Act. Indeed, proposals 11.1 and 11.3 simply formalise in legislation matters already contained in the Information Commissioner's APP guidelines. For that reason, these reforms should be uncontroversial and straightforward to take up.

Fair and reasonable test

Currently the Privacy Act offers little direction on the uses an entity may make of personal information, except that the information must be necessary to a defined use and should not be used for other purposes except in certain prescribed circumstances. This gives considerable latitude to entities and leaves open the possibility that entities use information for activities that do not meet community expectations.

We support the introduction of a fair and reasonable test into the Privacy Act for the reasons outlined in the Report (particularly those set out in section 12.2 (p 111)). Therefore, we **strongly support** proposals 12.1, 12.2 and 12.3.

In particular, we would like to underline the importance of proposal 12.3 which states that the fair and reasonableness test should apply irrespective of whether consent has been obtained. Without this condition, the test would be seriously weakened and entrench problems with the existing regime in which an individual can 'consent away' their rights to fair information handling.

Direct marketing, targeting and trading

The Report proposes several reforms to regulation of direct marketing, targeting and information trading. We **support** those proposals (the series 20 proposals).

With regard to 'targeting', proposal 20.3 would provide individuals with an unqualified right to opt-out of receiving targeted advertising and proposal 20.8 would require targeting to be fair and reasonable. Both are important though will only be successful and achieve their objectives if proposal 20.1 is implemented as outlined. That is, targeting must cover personal, deidentified and unidentified information. Without this, regulations applying to targeting will fail to address the growing impact of 'individuation' whereby individuals are tracked and targeted but the tracking and targeting falls outside the operation of the Privacy Act because the information involved is ostensibly 'deidentified'. Hence, the importance of proposal 20.1 and its definition of targeting.

We further submit that proposal 20.8 should remain broadly framed – that 'targeting' be fair and reasonable in the circumstances – rather than being narrowed in any way (for example, to require only that 'targeted *advertising*' be fair and reasonable). Naturally, a narrowing of this kind would weaken the effect of the fair and reasonable test as it operates in this context.

Enforcement and regulator funding

In general, we agree with reforms that would give the Information Commissioner greater flexibility in imposing civil penalties. Therefore, we **support** proposals 25.1 and 25.2. However, introducing enhanced or more flexible enforcement arrangements will be meaningless if the regulator – the OAIC – continues to be under-resourced.

In our submission to the Discussion Paper, we called for adequate resourcing of the OAIC which struggles to meet demand for its services even before any possibility of seeking court interpretation or enforcement. We repeat that call here. The digital economy has undergone massive expansion over the past decade and the privacy regulator must be appropriately resourced to keep pace, especially in the face of likely challenges from well-resourced entities. In an economy heavily geared towards the ingestion and use of personal information, enforcement of the responsibilities borne by regulated entities, along with individual privacy rights and avenues for redress, are more important than ever.

Proposal 25.7 of the Report recommends further work to investigate the effectiveness of an industry funding model for the OAIC. This approach runs the risk of heavy lobbying by regulated entities to limit funding obligations in order to minimise costs and weaken the regulator. We **agree in principle** with proposal 25.7 and on balance are not averse to an industry funded approach so long as adequate safeguards are in place to ensure adequate funding.

In a similar vein, we **support** the establishment of a contingency litigation fund to fund any cost orders against the OAIC and an enforcement special account to fund high-cost litigation, as foreshadowed by proposal 25.8. Reforms throughout the Report would introduce many new terms that stand on their 'ordinary meaning'. Some may even be highly contested, such as 'fair and reasonable'. Hence, they are only likely to be given accurate interpretation in the courts. This could be very costly for the OAIC if it is up against extremely well-resourced local and global companies.

Our remaining concern is that proposals 25.7 and 25.8 are framed in terms of 'further investigation' and 'further consideration' rather than a clear call to action. As such, those proposals risk being deprioritised or languishing in a state of uncertainty.

Appropriate funding for the OAIC cannot wait.

It is imperative that the Government acts immediately on the appalling discrepancy between the size of the challenge facing the OAIC and the resources at its disposal to meet that challenge.

Authors

Malcolm Crompton AM, FAICD, CIPP

Founder and Partner
mcrompton@iispartners.com | +61 407 014 450

Nicole Stephensen, FAISA, SCCISP

Partner
nstephensen@iispartners.com | +61 433 688 118

Natasha Roberts

Principal Consultant
nroberts@iispartners.com

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia

www.iispartners.com