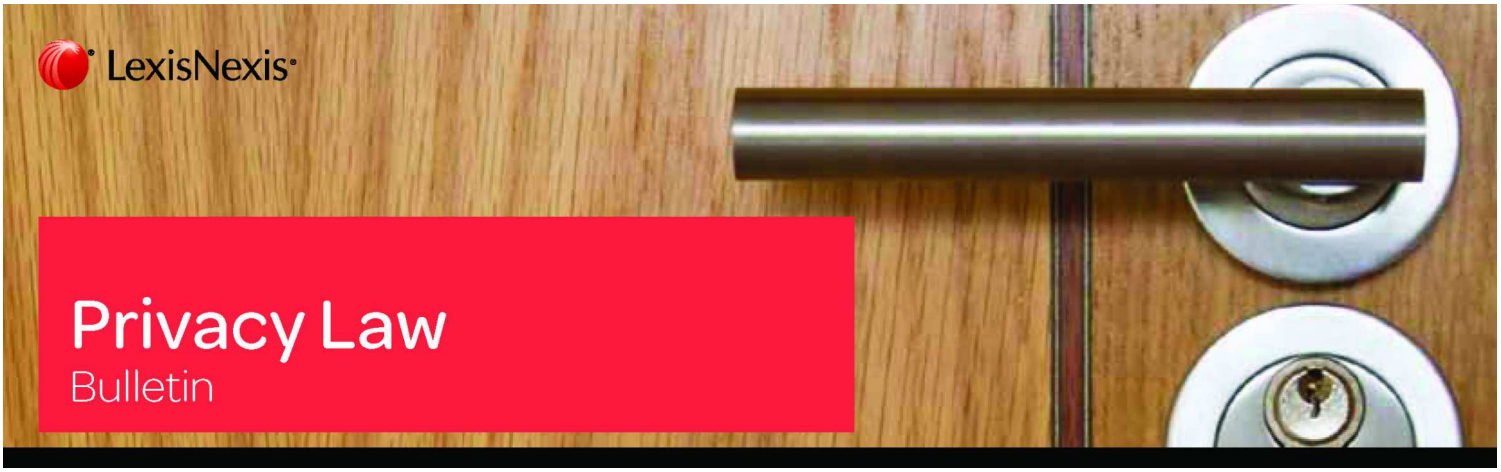

# Privacy Law Bulletin

2021 . Vol 18 No 2

## Contents





*Information contained in this newsletter is current as at May 2021*

LexisNexis® Butterworths

# Certain Privacy Act exemptions on the chopping block

***Dr Ashley Tsacalos*** *and* ***Monique Azzopardi*** *CLAYTON UTZ*

## Introduction

In response to the concerns raised by the Australian Competition and Consumer Commission in its *Digital Platforms Inquiry*,[1] the Australian Government is currently undertaking a review of the Privacy Act 1988 (Cth) (Privacy Act). In October 2020, the Attorney-General's Department released the *Privacy Act Review: Issues Paper* (Issues Paper).[2]

The Issues Paper considers whether the scope of the Privacy Act and the enforcement mechanisms contained therein remain fit for purpose, especially in today's digital economy. Among other matters, the Issues Paper considers the suitability and scope of certain exemptions under the Privacy Act, including the employee records exemption, the small business exemption, the political exemption and the journalism exemption. This article will focus on the scope of the employee records exemption, including the discourse surrounding whether employees' records should remain exempt from the protections and obligations under the Privacy Act. It will also consider the implications of removing or narrowing the scope of the employee records exemption.

## The employee records exemption

The employee records exemption was introduced in 2000 when the application of the Privacy Act was extended to the private sector. The exemption is contained within s 7B(3) of the Privacy Act. Its effect is that organisations subject to the Privacy Act are exempt from complying with the Australian Privacy Principles (APPs) if their acts or practices are directly related to:

- a current or former employment relationship between the employer and the individual and
- an employee record held by the organisation and relating to the individual

An "employee record" is defined under the Privacy Act as a record of personal information relating to the employment of an employee, including (among other categories of information) employee health information, information relating to the employee's performance, banking affairs, training, discipline and the employees' terms and conditions of employment.[3]

While, at first blush, the scope of the employee records exemption may seem wide-reaching, it is important to note the following:

- The exemption is not a general carve out and only applies to employees of an organisation. Therefore, it does not apply to contractors, subcontractors, volunteers or prospective employees (for example, job applicants).
- For the exemption to apply, there must be a sufficient nexus with the employment relationship. The exemption cannot be used as an excuse by private sector organisations to adopt a cavalier, lax or exploitative attitude to the handling, use or disclosure of employee records. For example, employers could not use the employee records exemption to commercialise employee personal information by selling it to third parties.
- The employee records exemption does not apply to "agencies" as defined under the Privacy Act. This means that public sector entities, such as agencies within the meaning of the Public Service Act 1999 (Cth), Commonwealth bodies, Federal Courts and Ministers are bound by the Privacy Act in relation to their handling of employee records.

In addition, recent case law from the Full Bench of the Fair Work Commission has narrowed the application of the employee records exemption to apply only to records that are already held by an employer, not to records that are yet to be created and held by an employer.[4] The effect is that the privacy collection and notice requirements under the APPs continue to apply in relation to employees. However, this matter was a decision of the Full Bench of the Fair Work Commission and was principally concerned with whether an employee had been unlawfully dismissed. The case has yet to be followed by a superior court and accordingly there remains a degree of uncertainty about its application from a Privacy Act perspective.

The inclusion of the employee records exemption in the Privacy Act has been justified in the past on the basis that the handling of employee records is a matter better addressed under workplace relations legislation. It has previously been argued that dealing with employee records under the Privacy Act would "create a confusing mosaic of obligations" when there are already interactions with other laws, including workplace relations laws.[5]

## Concerns with the ambit of the exemption

The Issues Paper has articulated concerns with respect to the current ambit of the employee records exemption and has prompted discussion about whether it should be removed or narrowed in part.[6]

The Office of the Australian Information Commissioner (OAIC) has recently announced its support for the removal of the employee records exemption "subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act".[7]

In its submission in response to the Issues Paper, the OAIC noted that, from a general perspective, the ongoing inclusion of certain exemptions under the Privacy Act is out of step with the privacy risks that have emerged over the last 20 years. The OAIC concluded:

> . . . it is no longer justifiable to exempt major parts of the economy from the operation of the [Privacy] Act. Personal and sensitive information held by small businesses, employers and political parties is not immune to the substantial risks that exist in the digital environment.[8]

In relation to the employee records exemption specifically, the OAIC highlighted that:

> . . . removing the exemption will address the risks posed to the personal information of employees and create benefits to employers by increasing trust and confidence in their personal information handling practices and addressing regulatory uncertainty about the scope of the exemption.[9]

The OAIC also highlighted that there is an important policy objective to ensure that an individual's personal information is protected to the same standard whether they are employed in the public or private sector and noted that the OAIC's *Australian Community Attitudes to Privacy Survey 2020* showed that 73% of Australians agree that businesses collecting work-related information about employees should be required to protect personal information in the same way that government is required to do so.[10] The OAIC also raised reservations about sole reliance on workplace relations legislation in relation to employee records.[11]

Calls for the employee records exemption to be removed from the Privacy Act are not new. Over 10 years ago, submissions to the Australian Law Reform Commission (ALRC) in response to the 2008 review of the Privacy Act identified that employers may accumulate a considerable amount of personal information about their employees, including sensitive information. There is potential for employees to be harmed if such information is used or disclosed inappropriately.[12] The ALRC also identified stakeholders' concerns that there are gaps in the legislative protection of employees' privacy and limited privacy protection provided by workplace relations legislation.[13]

## Implications of removing the employee records exemption

The removal of the employee records exemption will place Australia's privacy regime more in-line with comparable international regimes, including the European Union's General Data Protection Regulation (GDPR). The GDPR is frequently cited as the "gold standard" for privacy. Removal of the employee records exemption may also support the cross-border transfer of personal information between jurisdictions subject to the GDPR and Australia. This is because, under the GDPR, personal data can only be transferred outside of the European Union to countries that provide an adequate level of privacy protection. The European Commission has the power to determine whether a country outside the European Union offers an adequate level of data protection. Therefore, removal of the employee records exemption (along with certain other exemptions under the Privacy Act) may facilitate the recognition by the European Commission of the adequacy of Australia's privacy laws.[14]

The OAIC contends that, if the employee records exemption is removed from the Privacy Act, the compliance cost for employers would be relatively low. Further, the OAIC has stated that the compliance burden on employers to determine whether or not the Privacy Act applies is greater than having the Privacy Act apply to all personal information (including employee records) that the business holds.[15] We acknowledge that this will hold true in many situations. We further note that most businesses already safeguard employee records as part of good business practice. In addition, multi-national employers (for example, those subject to the GDPR) will, in many situations, already be required to deal with the personal information of their employees as they would any other category of personal information.

Employees also have other protections at law. Employers have existing common law duties of care and confidentiality as well as other legal obligations to their employees, including under workplace surveillance legislation. These laws also provide some information protections for employees.

However, given the significant amount of personal information (including sensitive information) that many

employers collect about their employees, if the employee records exemption was removed or narrowed, there will be (at least initially) an additional burden as well as additional compliance costs placed upon employers, especially from a human resources perspective. In this scenario, private sector organisations subject to the Privacy Act would need to ensure that their practices and procedures are sufficient from a compliance perspective. Such organisations will also need to ensure that human resource personnel and other personnel within their organisation dealing with employee personal information are trained in relation to their privacy obligations concerning employee records.

A particular issue for employers to navigate is the issue of consent under the Privacy Act in the context of employees. The Issues Paper has identified that there can be a power asymmetry in employee and employer relationships and that the ability for employees to provide genuine and voluntary consent may be limited. For example, consent may be vitiated by the threat (whether real or perceived) that employees may face disciplinary action if their consent is not given to their employer.[16]

From a legal and policy perspective, the Commonwealth may need to clarify and re-examine how employee records are addressed in the context of Australia's employment and workplace laws. In this regard, it will be important to ensure that there is no potential for duplication within the Australian regulatory and legal framework concerning employee records.

Finally, it is important to note that the removal of the employee records exemption cannot be looked at in isolation from other proposed reforms to the Privacy Act. As noted above, the Issues Paper also considers the appropriateness and scope of other exemptions under the Privacy Act, including the small business exemption. The cumulative effect of removing or narrowing the employee records exemption, along with other proposed Privacy Act reforms, has the potential to affect a greater number of private sector businesses.

## Conclusion

The current discussion about reforms to the Privacy Act represents a timely opportunity for private sector entities to re-examine their privacy practices and procedures. Regardless of whether the employee records exemption is removed or narrowed at a statutory level, private sector entities should see whether there are areas within their organisation that could be improved to ensure that there are no potential privacy or cybersecurity vulnerabilities in relation to the way they handle, process and protect their employee's personal information.

Privacy, and the protection of personal information, is not simply a legal matter. It is also a public relations matter and will assist the private sector in building trust and confidence among their employees. In turn, such trust and confidence may extend to the trust and confidence of an organisation's clients and customers that they are an organisation that takes privacy seriously — regardless of whose data it relates to.

***Dr Ashley Tsacalos***
*Partner*
*Clayton Utz*
*atsacalos@claytonutz.com*
*www.claytonutz.com*

***Monique Azzopardi***
*Senior Associate*
*Clayton Utz*
*mazzopardi@claytonutz.com*
*www.claytonutz.com*

## Footnotes

1. Australian Competition and Consumer Commission *Digital Platforms Inquiry* Final Report (June 2019).
2. Attorney-General's Department *Privacy Act Review: Issues Paper* (October 2020).
3. See Privacy Act 1988 (Cth), s 6(1) of the for the full definition of an "employee record".
4. *Jeremy Lee v Superior Wood Pty Ltd* (2019) 286 IR 368; [2019] FWCFB 2946, at [55]–[56].
5. Cth Hansard, House of Representatives, 8 November 2000, p 22370.
6. Above n 2, at 29–32.
7. A Falk, *Privacy Act Review — Issues Paper: Submission by the Office of the Australian Information Commissioner* (11 December 2020) 64.
8. Above n 7, at 58.
9. Above n 7, at 62.
10. Above.
11. Above n 7, at 63.
12. Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* Report 108 Vol 2 (May 2008) 1374.
13. Above, at 1374–1375.
14. Above n 2, at 32.
15. Above n 7, at 63.
16. Above n 2, at 32.

# Harder, better, faster, stronger? The possible future of the Notifiable Data Breach Scheme following the Privacy Act Review

***Alec Christie*** *and* ***Alexander McGuire*** *CLYDE & CO*

## Introduction

The Privacy Act 1988 (Cth) (Privacy Act) and the Office of the Australian Information Commissioner (OAIC) were, for some time, considered "toothless tigers", providing lacklustre consumer protections, minimal obligations for private entities and meek regulatory enforcement powers that lagged behind comparable jurisdictions. But, over the past 5 years, the Privacy Act has seen significant reform and the OAIC has developed such that Australia is now closer to its foreign counterparts. Much of this is attributable to the commencement of the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (NDB Scheme). This increased accountability of entities regulated by the Privacy Act, requiring that they report data breaches involving unauthorised access to personal information capable of causing serious harm.

This is now further bolstered by the Attorney General's Department announcement in December 2019 of a significant Review of the Privacy Act (Review). The Review is wideranging and has the potential to result in significant amendments to the Act, including in relation to the "new" Notifiable Data Breach Scheme (ie the NDB Scheme).

Impacting on the NDB Scheme, the Review is considering:

- expanding the definition of personal information
- the removal of various "exemptions" to the Privacy Act
- specifying stricter and clearer timelines for notification and
- introducing NDB Scheme related enforcement powers available to the OAIC

The Review closed for submissions on 29 November 2020 and received over 150 submissions.

## Context: the current NDB Scheme

The number of data breaches notified to the OAIC has increased each year since the introduction of the Scheme in 2018, and the introduction of the NDB Scheme itself increased the number of OAIC notifications 10-fold.

It is also widely accepted that the COVID-19 pandemic has increased instances of cyber-crime,[1] which will in turn also increase notifications. Threat actors are becoming more sophisticated, better resourced and increasingly ruthless. Recent months have seen increased numbers of ransomware, business email compromise and other headline-grabbing incidents such as SolarWinds and Microsoft Exchange. As a result, it is only a matter of time before we see increased notifications under the NDB Scheme.

Australia's regulatory and legislative approach to the privacy risks of cybercrime has improved in recent times. However, it is still far behind the requirements of the General Data Protection Regulation (GDPR) regime and other comparative jurisdictions and is in dire need of revamping. The current NDB Scheme applies to all entities that are subject to the Australian Privacy Principles (APPs) (ie those regulated by the Privacy Act). Small businesses, State governments and their agencies, to name a few, are exempt from complying with the APPs or the NDB Scheme (except in relation to Tax File Numbers).

A data breach is notifiable to the OAIC and all affected individuals if it meets the following three criteria:

- the breach involves unauthorised access to, disclosure or loss of personal information
- that access, disclosure or loss is likely (defined as more probable than not) to result in serious harm (undefined) to any individuals and
- there is no "remedial action" that can be (and has been) taken before any harm occurs to prevent the likely risk of that harm occurring

## Expanding the definition of "personal information"

The Review is considering expanding the definition of "personal information" in the Privacy Act, which is

currently limited to information, whether that information is true or not, *about* an identified or identifiable individual. This definition is more limited than the GDPR definition of "personal data" which includes information *relating to* an individual.

A narrow reading of personal information was given impetus by the Full Federal Court of Australia's decision in *Privacy Commissioner v Telstra Corp Ltd*,[2] which held that metadata and technical identifiers do not have the requisite personality to be covered by the Act. That is, the current definition, arguably, does not cover technical information such as IP addresses and geolocation data (of things especially) and that compromise of such data even if capable of causing serious harm to an individual, does not require notification under the NDB Scheme.

A significant majority of the submissions to the Review advocate for the expansion of the definition of personal information. While the submissions were varied, some of the more common suggestions included:

- a more explicit and exhaustive definition
- clarification that technical data is included in the definition
- consistency in the legislative definitions across different jurisdictions of terms such as "personal information", "sensitive information" and "health information"
- clarifying that the definition applies whether the information or opinion is provided, collected, created, generated or inferred and
- bringing the definition of "de-identification" into line with the GDPR and other jurisdictions

However, not all are so enthusiastic about such an expansive definition. CrowdStrike, a forensic investigation vendor that would arguably stand to gain business from an expanded definition, opposed it:

> Expanding this definition to include "inferred personal information" would likely introduce ambiguity in practice without expanding actual protections beyond the already-broad scope of the existing definition.

We believe unequivocally that a clearer, more progressive and future-proof definition of personal information is required, especially for the purposes of determining which incidents will require notification under the NDB Scheme. Expanding the definition of personal information will result in a host of incidents, previously not requiring notification, being brought within the scope of the NDB Scheme, incidents that normatively deserve notification.

## Removal of exemptions to the Privacy Act

Perhaps one of the biggest proposed changes to the Privacy Act is the removal of two of the main exemptions that businesses currently rely on to avoid complying with the Privacy Act, including:

- the "small business exemption" which absolves businesses with less than $3 million annual revenue from complying with the Privacy Act and
- the "employee records exemption" which absolves entities (even if otherwise covered by the Privacy Act) from complying with the APPs in respect of their employee records

### *Small business exemption*

The submissions are something of a deafening chorus in favour of removing the small business exemption. This proposition has rightfully attracted particular attention given its removal would bring over 2 million small businesses (representing 95% of Australia's total businesses by number) under the ambit of the Privacy Act for the first time and into the jaws of the NDB Scheme requirements.

The rationale behind removing the exemption is simple: the reasons for its existence in the first place are irrelevant and outdated. The exemption was devised in 2000 when the Privacy Act was expanded to the private sector as it was anticipated that small businesses:

- would not be able to cover the costs of complying with the Privacy Act if it applied and
- do not hold enough relevant personal information to justify the Privacy Act applying to them

The digitisation of business and society has not only revolutionised the amount of personal information that small businesses collect and use but has also reduced the costs associated with the proper handling of such data.

Small businesses are also increasingly being targeted by cybercrime. Some may assume that cybercriminals have "bigger fish to fry" but it is undeniable that small businesses are still targeted and compromised frequently as the "low hanging fruit". The reasons for this are 2-fold:

- small businesses have significantly weaker cybersecurity measures and are generally easier to breach and
- small businesses are now more "data-rich" than ever, making them worthy of targeting

Small businesses are often victim to both targeted and random (ie opportunistic) ransomware campaigns, resulting in them being extorted to avoid loss of sensitive or commercially valuable data. These campaigns often begin by users naively clicking malicious links or attachments sent through by threat actors (ie "phishing"). Clicking these links invites in malicious code and scripts known as the ransomware "payload" into the

network environment. The ransomware then begins to "encrypt" or lock as much information as it can reach, depending on the extent of the breach and the business' cyber security measures. The effect of this is that the business cannot access their information unless they engage in negotiations with the threat actor, who will often leave a "ransom note" requesting payment in cryptocurrency to provide the "decryption key" that will return their files to usability.

A growing concern with the rise of ransomware is that data is no longer just being encrypted *in situ* but is increasingly being "exfiltrated". That is, taken out of the network environment by threat actors for publication, misuse or further extortion. Ransomware is just one of the many common threats that face small businesses and justify the removal of the exemption: cybercriminals do not discriminate based on the size of the business and neither should the law (in particular the NDB Scheme). Just because one's sensitive information is collected and held by a small business, why should it be any less worthy of protection?

### *The employee records exemption*

The employee records exemption provides that any acts done by employers are exempt from the Privacy Act if those acts are directly related to the employment relationship with a current or former employee.

In practice the OAIC has recently relied on some creative statutory interpretation to argue that, while the information in question may be an employee record (and otherwise exempt from the Privacy Act), data breaches containing employee records are not exempt because they do not involve an act or practice engaged in by the employer organisation directly related to the employment relationship.[3]

We expect that the Privacy Act will be amended to resolve the regulatory and legislative tension here by removing the exemption altogether. The justification for removing this exemption, echoed in many of the submissions, is clear: employee records often contain sensitive personal information so exempting them from the operation of the Privacy Act is counterintuitive and counterproductive to the purported aim of the Privacy Act. That is, to protect the privacy of individuals in Australia.

It also exposes individuals (ie employees) to greater risk, prevents the OAIC from investigating "employee records" incidents and removes accountability for entities to investigate and report on breaches involving employee records. Under the current NDB Scheme (at least in the way the law is written), for example, if an entity is subject to a ransomware campaign similar to that described above, they are, at least by law, not currently required to make notifications under the NDB Scheme, even if there is clear evidence that sensitive personal information is in the hands of a threat actor.

According to the OAIC's *Australian Community Attitudes to Privacy Survey 2020*,[4] the removal of both the small business and employee records exemptions is supported by 71% and 73% of respondents respectively. Again, why should the personal information of employees be less worthy of protection?

For many of the small businesses that would be caught by the Privacy Act if the small business exemption was removed, the only personal information capable of misuse causing serious harm will be the identification and financial information of employees provided during HR onboarding. To that end, we believe that the simultaneous removal of the small business exemption *and* the employee records exemption will rightfully significantly increase the coverage of the NDB Scheme and thus the number of notifiable incidents.

## Notification timeline and OAIC's enforcement of the regime

The Review has also called for submissions in respect of the impact and efficacy of the NDB Scheme itself, including in relation to the timeline for when notification is required and the enforcement powers available to the OAIC.

The OAIC submission recommends that the NDB Scheme be amended to clarify that once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach then they must notify the Commissioner "as soon as practicable". However, the OAIC also state that this assessment and notification should, in any event, take no longer than 30 days in circumstances where the entity only becomes aware that there are reasonable grounds to suspect (ie not to believe) that there may have been an eligible data breach.

The OAIC also advocates for the NDB Scheme to clarify that an entity must notify individuals as soon as practicable, but no later than five days after notifying the OAIC. This submission means that in practice, if entities only suspect there may have been an eligible data breach, they must notify individuals affected by the incident, at the latest, 35 days after becoming aware of a possible incident. Further, the OAIC recommends that its enforcement powers be expanded so that they can issue infringement notices or apply to the courts for civil penalties in situations in which entities have failed to comply with these prescribed timeframes.

While clarity is certainly needed in respect of the NDB Scheme notification timeline, we suggest that the OAIC's submissions miss the mark. After assessment of

an incident, even though it might be clear that an NDB is likely to have occurred, it may still be unclear which individuals will require notification as a result.

Picture, for example, an incident in which a threat actor has accessed a large network environment containing millions of files, some of which are suspected of containing personal information that could be misused in a way capable of causing serious harm. The attacked entity is then tasked with commencing a forensic investigation to determine the extent of the access and/or exfiltration to assess which documents containing personal information are involved. Following this, they need to determine (on a case by case basis) whether the access to or exfiltration of each individual's personal information is likely to cause serious harm. While the process of finding and transcribing relevant documents is largely automated, there is still a large degree of manual review required for accuracy, sense-checking and transcription to ensure individuals receive an accurate and bespoke notification. It is inconceivable that this process can fully occur within 35 days in every circumstance, especially considering the degree to which systems can be affected by cyber-attacks.

Additionally, we believe the threat of the OAIC's proposed NDB Scheme enforcement powers will encourage rushed assessments which may lead to incorrect, irrelevant or misconceived notifications. The need for clarity in respect of the timeframes must be balanced with what can be reasonably expected of entities, especially given the potential for 2 million further smaller businesses having to comply with the NDB Scheme.

OAIC's current enforcement powers, which we believe are satisfactory as is, include the ability to:

- accept enforceable undertakings and bring proceedings to enforce an undertaking
- make determinations and bring proceedings to enforce a determination
- seek injunctions to prevent ongoing activity or a recurrence and
- apply to court for a civil penalty order for a breach of a civil penalty provision for a serious or repeated interference with privacy

OAIC's responsibilities are sure to increase as reforms are enacted over time. However, perhaps the best way forward is not to increase the enforcement powers available to OAIC, but rather to increase its funding to the OAIC to facilitate greater oversight of the NDB Scheme and to provide assistance to the likely 2 million small businesses which will become subject to the NDB Scheme for the first time.

## Conclusion

The Review is set to spawn significant reforms and enhancements to the NDB Scheme. We believe that, in particular, the expansion of the definition of personal information, the removal of the exemptions to the Privacy Act and clearer timing requirements for compliance with the NDB Scheme on the basis noted above are the best ways to strike the balance between moving the protections and compliance forward without becoming so difficult as to be counterproductive.

***Alec Christie***
*Partner*
*Clyde & Co*
*Alec.Christie@clydeco.com*
*www.clydeco.com*

***Alexander McGuire***
*Law Graduate*
*Clyde & Co*
*Alex.Mcguire@clydeco.com*
*www.clydeco.com*

## Footnotes

1. Office of the Australian Information Commissioner (OAIC) *Notifiable Data Breaches Report* (July to December 2020) 7.
2. *Privacy Commissioner v Telstra Corp Ltd* (2017) 249 FCR 24; 347 ALR 1; [2017] FCAFC 4; BC201700165.
3. A Christie "Do You Need To Notify A Data Breach Impacting 'Employee Records'?" *Clyde & Co* 16 March 2021 www.clydeco.com/en/insights/2021/03/do-you-need-to-notify-a-data-breach.
4. OAIC *Australian Community Attitudes to Privacy Survey 2020* (September 2020).

# Under construction: a direct route to enforcing privacy

***Andrea Beatty**, **Chloe Kim** and **Shannon Hatheier** PIPER ALDERMAN*

A survey conducted by the Office of the Australian Information Commissioner (OAIC) revealed that privacy is a major concern for 70% of Australians, and 9 in 10 want greater control over their personal information.[1] The findings raise serious questions as to whether the current legislative framework effectively protects the right to privacy and promotes good privacy practices. In an attempt to address this concern, a review of the Privacy Act 1988 (Cth) (Privacy Act), conducted by the Attorney-General's Department, proposed in its Terms of Reference a direct right of action to enforce privacy obligations under the Privacy Act. Following this, the Attorney-General's Department released an Issues Paper considering whether the scope of the current Privacy Act and its enforcement are fit for purpose. A significant matter for consideration is the implementation of a direct right of action.

## Current framework

The Privacy Act currently does not provide a right of action enabling individuals to pursue a breach of privacy principles directly actionable in court. Accordingly, individuals are required to make a complaint to the Privacy Commissioner (Commissioner) of the OAIC who has the power to make a determination in relation to the complaint. Under s 52 of the Privacy Act, the Commissioner has the discretion to issue a declaration that the respondent:

- not repeat or continue the conduct
- perform any reasonable act to redress any loss or damage suffered
- take specified steps to ensure the conduct is not repeated or
- pay a specified amount to compensate the complainant for any loss suffered

Complainants may subsequently apply to the Federal Court or Federal Circuit Court for an order enforcing the Commissioner's determination. However despite this, in the case of *Day v Lynn*,[2] her Honour described the jurisdiction of the court in relation to breaches of privacy as limited to circumstances only where a determination has been made by the OAIC Commissioner or where individuals are seeking an interim injunction pending a determination.[3] Absent an application to the Federal Court or Federal Circuit Court, determinations of the Commissioner are not binding or conclusive between the parties.

## A direct right of action

A direct right of action would provide a legislative basis for individuals to directly apply to a court for a determination as to whether an entity regulated under the Privacy Act has acted in breach of its provisions and obtain an order for compensation. A direct right of action refers to a person's right to begin and prosecute an action in the courts for the purpose of enforcing a legal right and obtaining compensation. Cognisant of the potential for trivial breaches of the Privacy Act to unnecessarily burden the court's resources, the Privacy Act Review proposed alternative frameworks for framing a direct right of action.

### *Attorney-General*

Firstly, the Issues Paper suggests limiting the direct right of action to only "serious" breaches of privacy. This approach would require the formulation of a harm threshold against which breaches are measured. However, this presents the issue of formulating a prescriptive criteria defining the necessary degree of harm to constitute a "serious" breach. A task complicated by the multitude of damage capable of being caused by a privacy breach including physical, psychological, emotional, financial, or reputational harm. Nevertheless, such conceptual difficulties will likely be clarified on a case by case basis and prove an effective means of diverting only the most serious cases to the court's forum.

### *OAIC*

The OAIC however argues that limiting the direct right of action to "serious" breaches of privacy would substantially curtail its effectiveness.[4] The OAIC maintains that such a limitation would diminish the degree of agency and control individuals are entitled to exercise over the handling of their personal information. Furthermore, the OAIC proposes a direct right of action similar

to Singapore's Personal Data Protection Act 2012, which provides a broad provision that any person who suffers loss or damage as a result of the Act has a right of action to seek relief in civil proceedings.

As an alternative to limiting a right of action to serious breaches, the Issues Paper proposed making conciliation by the OAIC or another administrative body either a mandatory or optional prerequisite to proceedings in an attempt to curtail the litigation of trivial breaches. The OAIC in response suggested an approach that does not require the Privacy Commissioner to conciliate where it believes the matter would more appropriately be dealt with by the court. A compromise could result in directing all complaints through the OAIC to apply a predetermined criteria for determining which matters are to proceed to court.

## A statutory tort of privacy

In addition to, or as an alternative to a direct right of action, it is suggested that a statutory cause of action for serious invasions of privacy be introduced. A tort of privacy was among the key recommendations in the Australian Competition and Consumer Commission's *Digital Platforms Inquiry* Final Report and was subsequently endorsed by the Australian Law Reform Commission, who described the cause of action as necessary to fill an increasingly conspicuous gap in Australian law.[5]

The proposal to introduce a privacy tort however is not a recent development but has been discussed at both state and federal levels for over a decade. In *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd*,[6] the court declined to recognise a cause of action for a breach of privacy, however suggested that it may be receptive to arguments in favour of a right to privacy in the future. An invasion of privacy tort, whether developed in statute or at common law, would enable individuals to apply for injunctions to prevent the misuse of personal information or alternatively grant victims a right to damages, which could include for emotional distress.

However, despite repeated and well-informed recommendations to do so, the Government has been reluctant over the past decade to enact such a tort. Following recent developments, such as the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018 (Cth), there are grounds to suggest that the matter is adequately dealt with under criminal law. An invasion of privacy tort is also likely to come into conflict with the constitutionally enshrined doctrine of freedom of press and expose media outlets to unnecessary liability.

## Damages

A direct right of action would entitle individuals to seek compensatory damages as well as aggravated and exemplary damages in exceptional circumstances for the financial harm suffered as a result of a breach of the Privacy Act. The OAIC in its response to the Issues Paper, further recommended expanding the scope of damages to non-financial loss to include harm such as humiliation and distress. It was also recommended that there not be a cap on compensation to enable the courts to develop standards for the levels of damages for privacy breaches on a case by case basis.

## Final thoughts

The findings of the Privacy Act review may well prove critical in deciding whether the legislature grants Australians the power to initiate court action and seek compensation for breaches of privacy. As businesses and platforms continue to expand online and increase their exposure to privacy breaches, it will become increasingly important to safeguard individuals' personal information and sensitive data. The recent acceleration in the number and sophistication of cyber attacks further emphasises the need for holders of personal data to proactively implement safeguards. If you would like to learn more about your obligations under the Privacy Act please contact the authors.

***Andrea Beatty***
*Partner*
*Piper Alderman*
*abeatty@piperalderman.com.au*
*www.piperalderman.com.au*

***Chloe Kim***
*Lawyer*
*Piper Alderman*
*ckim@piperalderman.com.au*
*www.piperalderman.com.au*

***Shannon Hatheier***
*Law Clerk*
*Piper Alderman*
*shatheier@piperalderman.com.au*
*www.piperalderman.com.au*

## Footnotes

1. Office of the Australian Information Commissioner *Australian Community Attitudes to Privacy Survey 2020* (September 2020) available at www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf.
2. *Day v Lynn* [2003] FCA 879; BC200305553.
3. Privacy Act 1988 (Cth), s 55A(3).
4. Office of the Australian Information Commissioner *Privacy Act Review Issues Paper Submission* (December 2020).
5. Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era* (June 2014).
6. *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1; [2001] HCA 63; BC200107043.

# Let's not reinvent the wheel: tried and tested independent certification schemes as the future of privacy assurance

***Alec Christie*** *and* ***Sian Pannach*** *CLYDE & CO*

The Attorney-General's review of the Privacy Act 1988 (Cth) covers multiple areas, including the desirability and feasibility of an independent certification scheme with an underlying "standard" or framework (ICS) against which to demonstrate compliance with Australian privacy laws. In practice this means that entities which meet an objective threshold, as independently certified under an approved ICS regarding the collection, use and disclosure of personal information, will be taken to have demonstrated compliance with the Australian Privacy Principles (APPs) and the Privacy Act (or, at the very least, established the good will/their earnest attempt to do so).

## Why a certification scheme?

The potential introduction of an ICS has been met with mixed reactions and little consensus. Some industry stakeholders have questioned whether an ICS is needed, how it would operate, whether it should be voluntary or mandatory and whether its benefits would outweigh the risks. However, other industry stakeholders see an ICS (if a globally accepted ICS is approved for Australia) as a means of lessening the barriers to the cross-border movement of data (ie, personal information). There is also the question of who would certify compliance with ICS — eg the Office of the Australian Information Commissioner (OAIC), an existing certification body or a vendor of the privacy framework?

With many questions yet to be answered and numerous perceived risks associated with introducing an ICS we propose that, rather than reinventing the wheel, Australia should look to an existing tried and tested ICS process that has already been effectively implemented, has a long track record, already has had significant take up in areas outside privacy and have assisted Australian businesses in the global market.

## Examples of existing, rigorously certified standards

### *ISO/IEC 27701*

The International Organisation for Standardisation (ISO) 27001 standard, on which ISO 27701 is built, takes a risk-based "information security management system" (ISMS) approach to the management of information security and is the most used cyber/information security standard adopted globally. ISO 27001 encourages organisations to identify information assets that are most important to their operations and provides a structured framework and set of controls for protecting the security of those information assets by implementing an appropriate ISMS.

ISO 27701 adds the privacy "layer" over the existing ISO 27001 ISMS requirements. ISO 27701 provides a structured framework for designing, implementing and continually improving a "privacy information management system" (PIMS). For those companies which have already obtained certification under ISO 27001, implementation of the PIMS under ISO 27701 will be very familiar territory. Organisations that become certified to ISO 27701 are, in practice, using the PIMS to comply with both their local privacy requirements and most of those jurisdictions (including General Data Protection Regulation (GDPR)) in which they operate or with which they wish to share data. The ISO 27000 series of standards and the associated certification framework has been around for many years and has the biggest uptake of any information security standard. That is, companies globally are already comfortable and familiar with them and the certification framework. Given many entities already comply with one or more of the ISO 27000 series, it is not a huge cost (in money or effort) to add a PIMS under ISO 27701 over the top of their ISMS. As an international standard ISO 27701 also provides enough flexibility to cater to jurisdictional variations. Our experience suggests that the ISO 27701 privacy standard is (like its sibling information security standard ISO 27001) fast becoming the front-runner as the *de facto* global standard for privacy.

Certification under ISO 27001 (having an ISMS) is a prerequisite for certification under the ISO 27701 (and implementing a PIMS). This is perhaps one of the greatest benefits of the PIMS implemented under the ISO 27701 as it is built on a solid ISMS (ie, information security) foundation.

ISO 27701 certification is provided by a wide range of certification bodies independent of the regulator and the body that drafted the standard. In comparison with other frameworks, the ISO framework has been around for many years, and certification bodies and organisations seeking certification have familiarity with it. It is perhaps one of the few internationally recognised robust PIMS standards that is truly independent and part of a trusted and accepted certification framework.

Complying with ISO 27701 (ie, implementing the PIMS) provides the tools and procedures (ie, controls) to comply with the whole breadth of local and global privacy laws. For instance, if an Australian company was certified under ISO 27701 (ie, had implemented the relevant controls/requirements), and it was to expand operations to Europe, the existing PIMS framework could be scaled up and modified to meet the GDPR requirements.

ISO 27701 includes an annexure which maps its controls directly to the GDPR requirements. ISO 27701 also closely maps to the privacy laws in a number of other jurisdictions (including Australia) as shown (and explorable) in the Microsoft Privacy Mapping Project,[1] now maintained by the International Association of Privacy Professionals (IAPP). Having assisted Microsoft with this project, we are convinced that the ISO 27701 controls align very closely with Australian and other regional privacy laws.

While ISO 27701 is yet to be approved as an ICS by the European Data Protect Board (EDPB), we expect that this is only a matter of time. We understand that, once approved that the EDPB or DPAs would determine what additional or special (ie over the top) requirements will be needed in order for certification under ISO 27701 to be considered as evidence of GDPR compliance. We suggest that this is an approach the OAIC could take in relation to adoption of ISO 27701 as an approved ICS in Australia. If accepted in the European Union (EU) and by Asia-Pacific regulators, ISO 27701 certification could then be considered as a "white list" of sorts between the EU and our region.

### *SOC 2*

SOC 2 is less comprehensive than the ISO 27000 family and ISO 27701 but is also widely used. Developed by the American Institute of Certified Public Accountants (AICPA), it defines criteria for managing customer data based on the five "trust service principles" of security, availability, processing integrity, confidentiality and privacy. SOC 2 compliance involves an independent "auditor" producing a Type I report (which describes a service organisation's systems and whether the design of specified controls meet the relevant trust principles) and/or a Type II report (which addresses the operational effectiveness of the specified controls over a period of time).

While SOC 2 allows some "wriggle room" to adapt practices to the specific attributes of any given organisation, it lays out a skeleton framework of the kinds of controls that need to be implemented across the organisation — in greater specificity than, for example, the current APPs.

### *GDPR*

The EU's GDPR has accepted the benefits of an ICS but, at present, the specific ICS, associated certification criteria and accreditation bodies are yet to be determined. However, ISO 27701 is clearly in the mix.

## Wheels that didn't have enough grease!

### *APEC Cross Border Privacy Rules System*

The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) establish a privacy assessment regime available to all 21 APEC economies (including Australia), although only eight have adopted it so far. Its assessment is considered less than robust (outsourced by tender and rarely involves the level of independent assurance of ISO 27701 or SOC 2) and implements the nine "APEC Privacy Principles" introduced in 2004. At best the CBPR reflects privacy standards of some 20 years ago, no longer matching the realities of today's digital economy.

As well as poor country take up, the CBPR holds a poor track record for industry take up. The framework has been of no domestic significance in most APEC economies, even in those that have implemented it. In jurisdictions that have signed up, the level of protection afforded by their general privacy law often far exceeds that of the CBPR/APEC Principles. In practice this means "Accountability Agents" certify against the much lower bar of the APEC Privacy Framework, rather than against the standard of the national laws of the entities certified.

### *EU/US Privacy Shield*

The Privacy Shield (and Safe Harbour before it) is another example of a government-to-government self-certification style scheme which does not work, given it has been struck down again. Issues about its effectiveness were raised from the start and these fears were confirmed in the *Schrems II* case[2] where the European Court of Justice struck down the shield on the ground that invasive US surveillance programs were violating fundamental EU privacy rights, irrespective of any

"certification" obtained by the US company. Five years before the very same court sunk its predecessor "Safe Harbor",[3] an arrangement that also promised protection of EU citizen data when transferred to "certified" US companies.

At their core, the Privacy Shield and Safe Harbour failed as these sorts of government-to-government schemes are inherently no longer fit for purpose. The lesson to be learnt is that, only by drawing on successful, established, globally accepted, and robustly independent (beyond reproach) certification of compliance with a rigorous underlying standard can an ICS deliver the privacy certainty businesses crave.

## Benefits of using an ICS framework already widely recognised

It is difficult, time consuming and resource intensive to build a standard and certification framework anew in each jurisdiction (perhaps only to have it struck down later). Unnecessary compliance effort and costs can be avoided by using the "wheels that already turn", that is, drawing on standards and independent certification frameworks that are already tried, tested, and trusted.

A commonly cited critique of introducing an ICS in Australia is the high cost and burden of compliance with that ICS. Thus, it should be voluntary and remain independent of the regulator and the body "selling" the framework and encourage competition between trusted certification bodies. There are also fears that the certification process becomes a meaningless, fee generating "tick the box" exercise, especially where the individual responsible is not supported to scope and manage the certification process or where the creator of the framework is also assuring its implementation (surely a conflict of interest). However, these risks are avoided by relying on an existing, appropriate, robust and independent ICS such as that offered by ISO.

### *Providing competitive advantage*

As almost every sector of the economy has embedded digital infrastructure into its core systems, in 2021 it would be remiss to ignore the emerging reality that national privacy regimes may be a barrier to cross-border trade for Australian companies, making it difficult to do business in some of our potentially largest markets.

In addition, technology innovators are always on the look-out for the best markets to develop their new ideas in. Australia is a "competitor" in a race to attract new talent and capital. One way we can compete is to establish a reputation for having a privacy framework that is simultaneously accommodative, robust and in which there is a way to leverage Australian compliance into other markets. This is much like how multilateral trade agreements improve merchandise flows and enrich Australians, the Australian digital sector will be better connected to the global digital market if we encourage our market participants to speak a common privacy *lingua franca*. An appropriate globally recognised ICS can do just that and ISO 27701 backed by the trusted ISO certification framework behind it is a very worthy candidate for consideration.

### *Demonstrating compliance to an organisation's customers*

The beauty of an appropriate ICS is that it is done once (ie, certified and renewed annually) but may be used to prove compliance to all of an organisation's customers in Australia and beyond. The market acceptance of an ISO certification makes it easier for Australian technology companies to develop products that are ready to scale up and to easily enter new markets around the world.

### *Overseas data flows and privacy interoperability*

Especially for global organisations, the international transfer of data (ie, personal information) is a reality of day-to-day business. Drawing on a pre-existing globally accepted ICS standard with trusted, robust and independent certification will facilitate greater overseas data flows and digital trade opportunities between those certified. Association of Southeast Asian Nations (ASEAN), for example, has already flagged ISO 27701 as a key element of their new Data Management Framework.

Having established an independently certified PIMS and controls which can be tweaked and adapted for those domestic privacy laws without "starting again", a company seeking to enter a new market will be extremely well placed. For instance, if an Australian business sought to expand its operations into France and Germany, its existing privacy PIMS under ISO 27701 could be tweaked to comply with the GDPR and may soon be recognised under the GDPR as one of the acceptable ICS schemes. This will reduce privacy compliance costs and enhance the ease of conducting a global business.

### *Indicates the prima facie position to the OAIC*

The independent certification to an approved ICS should be noted by the OAIC as an indicator of an organisation's *bona fides* if an incident were to occur. Preferably, in choosing an ICS, the OAIC will indicate how they will view certification to it (ie, what benefits as to their approach to compliance and enforcement arise from it). That is, if there were a data breach, for example, would certification mean the company is given the benefit of the doubt for such and lead to reduced fines and penalties, other things being equal?

### *Transparency for consumers*

Using an accredited independent ICS review body, as under the ISO regime for example, would provide a great deal of comfort to individuals and other businesses as to how the certified company is managing and protecting personal information. Having compliance with ISO 22701 audited and assured by the likes of accredited Big 4 "auditors" and other trusted organisations is clearly a certification robustness and thus a level of comfort that a self-assessment (or "tick-a-box") accreditation scheme cannot match.

## What an ICS needs to work

For an ICS to work for privacy compliance in Australia and for Australian based businesses, we suggest that it should:

### *1. Be on a voluntary basis*

In its submission to the ACCC's Digital Platforms Inquiry the Australian Privacy Foundation suggested a voluntary scheme would be inherently flawed, given the certifying body must "sell" the certification and imply it is relatively easy to obtain. Entities would be otherwise disincentivised by the risk of wasting money on failed certification attempts. However, as noted above, an existing trusted certification framework (eg, ISO) which is globally recognised will bring a wealth of benefits to individuals and businesses.

If the ICS is mandatory, concerns have been raised as to how to identify an "objective threshold" to determine which APP entities would be required to obtain independent certification to the ICS. A voluntary scheme would remove this concern and would ensure that those partaking in the scheme are focussing on the benefits of managing privacy.

Simply put, leave it to a system that works in many other areas (from quality control to cybersecurity). A voluntary scheme with robust certification, a great track record in other areas and a great quality standard underpinning it is much more likely to promote the sustainable and predictable protection of personal information while also, in many cases, uplifting privacy compliance and the standard of personal information management.

### *2. The standard or framework must be independently and rigorously certified*

An effective ICS must be:

- robust in its framework and its approach (i.e. the underlying standard) and
- guarantee a rigorous and independent assessment in order to be certified to it

Only this will ensure that corporate interests are not prioritised over consumer interests. In this sense, ISO 27001 and the established ISO certification process is the gold standard.

Further, if privacy compliance achieved is measured against the Privacy Act and APPs, as it is with ISO 27701, this sets a higher standard than the state sanctioned or regional certification schemes, such as the CBPR, which tend to the lowest common denominator.

### *3. Be approved by the OAIC but certified by others*

The OAIC should not carry out certification itself, it should remain independent. The ICS standard or framework to be implemented should also be independent from those certifying its implementation (in the same manner as ISO 27701 works). This will prevent any conflicts of interest between the framework, sales, certification and ultimate enforcement by the OAIC of any non-compliance with the APPs. Conflict concerns can also be addressed by insisting on objective criteria for certifying auditors and subjecting these auditors to occasional performance reviews by the OAIC. That is, like the existing ISO framework.

In addition, noted elsewhere, the OAIC is already severely under-funded and constrained by limited resourcing and setting up its own ICS framework may divert it from its "day job". Truly independent certification bodies for an approved ICS will allow the OAIC to focus on enforcing existing privacy law, managing the notifiable data breach (NDB) scheme and to be more proactive with initiating privacy investigations.

### *4. Benefits to certified entities to be clearly outlined by the OAIC*

The OAIC must nominate what ICS it will accept and explain its approach to certification to it. For example, to what degree would the OAIC recognise certification as a good faith attempt to comply with an entity's privacy obligations? If there was nevertheless a breach, by how much will certification reduce fines and damages (or what other benefits will follow)? These answers will provide clear incentives to many in the private sector to follow the certification path. Further, using a globally accepted ISO standard and existing trusted ICS certification framework will help cross border data flows and Australian businesses.

If an ICS approved by the OAIC achieves the above, organisations will realise that demonstrating privacy compliance is not just something that has to be done but is, in fact, a strategic business enabler.

## Conclusion

To be truly effective, an Australian approved ICS should be an existing globally respected standard with a

"beyond question" robust certification framework. In fact, there must be a built-in "guarantee" that the framework/standard and certification are independent, assessment for certification is rigorous and can be relied on (ie not a "tick-a-box" self-assessment).

We suggest that ISO 27701 is a worthy front-runner. Certification under ISO 27701 will "guarantee" the independent and rigorous certification against a globally recognised standard.

In this respect, we hope that the Review of the Privacy Act may be the grease that gets the appropriate ICS wheels turning for Australia.

***Alec Christie***
*Partner*
*Clyde & Co*
*Alec.Christie@clydeco.com*
*www.clydeco.com*

***Sian Pannach***
*Law Graduate*
*Clyde & Co*
*Sian.Pannach@clydeco.com*
*www.clydeco.com*

## Footnotes

1. Linkedin, Data Protection/Privacy Mapping Project, 2020, www.linkedin.com/company/dpmap/.
2. *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* C-311/18.
3. *Maximillian Schrems v Data Protection Commissioner Case* C-362/14.

# Review of the Privacy Act 1988: rethinking core concepts of privacy harms

***Peter Leonard*** *DATA SYNERGIES*

The Attorney-General Department's Review of the Privacy Act 1988 (Cth) provides an opportunity to reset the frame of reference for handling of personal information about individuals by Australian Privacy Principle (APP) entities.

The central problems with the Privacy Act are not as to coverage or comprehensiveness of the Act. There are deficiencies in coverage of the current Act, including overly broad exceptions and lack of clarity as to operation of the Act in relation to pseudonymised personal information and information relating to the use of devices by individuals that are not directly identifiable. These deficiencies need to be addressed in order to create appropriate incentives for APP entities to design and operate data ecosystems that embed minimisation of use and sharing of identifying information about individuals.

However, a more fundamental problem with the Privacy Act is the lack of clear implementation of its central purpose.

The objective of the statute is to create regulatory incentives and sanctions that cause APP entities to actively assess and mitigate risks of harms to affected individuals that otherwise might arise through the collection and handling of personal information about those individuals. Because of the lack of clear implementation of the central purpose of the statute, many APP entities adopt an episodic, form over substance, approach to the assessment of compliance with the statute, rather than embedding reliable data privacy assurance into their ongoing business processes.

The Privacy Act is not at all clear as to when privacy harms that impact individuals are of nature or magnitude that an act or practice should not be countenanced, regardless of notice to, or consent of, affected individuals. You can read the statute end to end and still have little idea of why or how an APP entity should assess and mitigate risks of privacy harms to individuals and manage residual risks.

The primary, and often exclusive, data privacy focus of APP entities is upon two things:

- mitigation of legal compliance risk and reputational risk and
- ensuring just enough transparency to meet requirements for notice and consent and comply with provisions of Australian Consumer Law

Impacts upon individuals of excessive collections, uses and disclosures of personal information have not been properly evaluated and addressed by many APP entities.

If the statute is appropriately restated, APP entities would have less scope to perceive that they could "paper their way to compliance", or use behavioural psychology to "game" requirements as to notice and consent.

There are four central problems in practical operation today of the Privacy Act that could be addressed by revisions to the Privacy Act, without a fundamental rewrite of the statute.

## Bringing organisational accountability into the frame of reference of APP entities

Accountability of entities handling personal information about individuals requires an appropriate regulatory framework to ensure that each entity:

- evaluates reasonably foreseeable risks
- mitigates these risks, through forbearing from certain acts or practices and taking appropriate steps (including appropriate technical, operational and contractual controls and safeguards, and disclosures) to address manageable risks
- manages residual risks

of significant privacy harms that individuals might reasonably be anticipated to suffer that arise from acts and practices of an APP entity itself, and of other entities within data ecosystems enabled or managed by an APP entity, in collecting, handling and disclosing:

- personal information about affected individuals (as currently defined) and
- non-directly identifying information about affected individuals that may be used to individuate (differentiate) that individual, or small cohorts of individuals, to affect a differentiated outcome that is reasonably likely to have a significant and adverse effect upon that individual

Redefining "personal information" to extend its coverage to capture device identifiers, tracking code and other information that relates to an individual is not appropriate, for so long as the associated obligations remain focussed upon notice and consent. Transparency does not of itself create more accountability: more information does not of itself create better knowledge and understanding of affected individuals, particularly as data handling practices become more technically complex. More disclosure may in fact increase information and power asymmetries between APP entities and affected individuals, by increasing the burdens placed upon individuals:

- to understand an APP entity's data handling practices
- to self-assess an individual's privacy concerns, tolerances and preferences
- to understand what options are available to the individual and
- to self-manage such privacy settings as they may be offered

We will achieve little more than collective exhaustion and loss of digital trust of citizens if the outcome of the Attorney General Department's Review is expansion of the definition of "personal information" and dialling up of requirements for notices and requests for consent. Notices and requests for consent will not be an effective control or safeguard for in many contexts of handling of personal information, regardless of however those notices and requests may be simplified, layered, targeted, made "just in time", made not misleading, and made plain English and "transparent".[1] Extending the definition of "personal information" within the current notice and consent framework will further expose the deficiencies in that framework and be unlikely to substantially change acts and practices of many APP entities in the collection and handling of information that can cause privacy harms to affected individuals. Organisational accountability should become part of the framework.

Consider by way of contrast Bill C-11, as introduced into the House of Commons of Canada in November 2020.[2] Clause 7(1) states "an organization is accountable for personal information that is under its control". The Bill then directly addresses the allocation of responsibility to a particular individual or role, to ensure that penalties are not just a cost to an organisation of doing business. Clause 8 states that:

> An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it.

The Bill then recognises that an organisation is unlikely to reliably and verifiably comply with the law unless it embeds good data privacy governance in everything that the organisation does, through a program of assurance. Clause 9 of the Bill states:

> (1) Every organization must implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil its obligations under this Act, including policies, practices and procedures respecting
>
> (a) the protection of personal information;
>
> (b) how requests for information and complaints are received and dealt with;
>
> (c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and
>
> (d) the development of materials to explain the organization's policies and procedures put in place to fulfil its obligations under this Act.
>
> . . .
>
> (2) In developing its privacy management program, the organization must take into account the volume and sensitivity of the personal information under its control.

Responsibility of an organisation in relation to its service providers is then addressed:

> If an organization transfers personal information to a service provider, the organization must ensure, by contract or otherwise, that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide under this Act.[3]

## Lack of understanding of many APP entities (both businesses and government agencies) as to why, how and when to assess risks of privacy harm impacts upon affected individuals

Fixing this problem requires much clearer guardrails in the Act, including:

- The Privacy Act should expressly address the key concepts of privacy risks and privacy harms.
- There should be certain "no-go zones", either statutory or by a declaration by the Commissioner (following proper public consultative processes), including behavioural advertising knowingly directed at younger children.
- There should be a requirement of (objective) reasonableness (appropriate purpose) in acts and practices of APP entities in the collection, handling and disclosure of personal information about individuals and other individuating information.
- There should be carefully crafted exceptions for legitimate interests (including reasonable business purposes), including (where this justification is clearly stated by an APP entity and is objectively reasonable) promotion of individual interests and societal interests.

As the Privacy Act does not clearly state when, why or how APP entities should assess privacy impacts upon individuals, it should not be surprising that APP entities focus upon formal compliance, and not privacy impacts.

Fixing this problem requires a restructuring of the front end of the Privacy Act, coupled with simplification in a statement of key requirements.

This restructure and restatement is now particularly important because data collection and handling are becoming more pervasive and intrusive and data privacy affecting acts and practices become common across a broad range of organisations.

This existing problem will also become more widespread if coverage of the Privacy Act is expanded to include small to medium enterprises (SMEs). The current Privacy Act is not sufficiently clear in its intended operation to be ready for the statute to apply to SMEs. Applying the Act in its current form will impose a significant regulatory burden on many entities that cannot reasonably be expected to properly understand and apply the statute. This burden could be substantially lessened if the Act is reframed.

There should be a clear statement that an organization may collect, use or disclose individuating information only for purposes that a reasonable person would consider appropriate in the circumstances. Considerations of reasonableness need to take into account a broad range of sensitivities, including concerns about:

- sensitive material exposed through data (such as health status, religion, gender orientation, geolocation, and interactions with other individuals)
- unexpected insights being generated from data leading to negative surprises or embarrassment of the data subject
- who may see or use insights generated from data
- the ability of a data holder to appropriately interpret analysis of that data (for instance, whether expert knowledge or additional context is required), whether or not due to poor data quality
- whether a data holder will apply data and analytical outputs to effect unacceptable outcomes, for example, through insights or decisions being poorly interpreted or applied (ie Robodebt)
- unintended consequences of analytical outputs to effect outcomes
- loss of agency (control) of the data subject
- problems of age of data (previously unexamined data, data which describes contemporary situations or data which was gathered in an environment which is no longer current and so outputs require new contextualisation)
- possible accidental release or other exfiltration of data and analytical outputs
- explainability of an action made based on an insight or decision from an analytical output
- reversibility (or not) of an action taken based on an insight or decision from an analytical output
- harm caused based on an insight or decision from an analytical output

## Many APP entities do not have ongoing data privacy management programmes. PIAs are often conducted as an audit style function, with the primary objective being reducing business risks of an APP entity, and not mitigation of privacy impacts upon affected individuals

Privacy risk management by many APP entities is episodic, often associated only with the commissioning of new projects and major changes that are subject to the formal change management process. Privacy impact assessments (PIAs) often are not conducted when they should be. PIAs often are conducted only when regulatory compliance people are called in, and not built into an APP entity's business processes and practices. PIAs often not revisited when an APP entity's everyday processes or practices in handling of personal information relevantly change.

Fixing this problem requires obliging APP entities to implement practical, ongoing, operational data privacy management programmes, not only to conduct PIAs for projects of high impact.

APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require "privacy by design", an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards. Conducting a Privacy Impact Assessment (PIA) may help an entity to ensure privacy compliance and identify better practice. A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.[4] However, the conduct of a PIA is not mandated by the federal Privacy Act.

The Privacy (Australian Government Agencies — Governance) APP Code 2017 (the Code)[5] requires Australian Government agencies subject to the Privacy Act to conduct a PIA for all "high privacy risk projects". The Code provides that a project may be a high privacy risk project if an agency reasonably considers that the project involves any new or changed ways of handling personal information that is "likely to have a significant

impact on the privacy of individuals".[6] The Guidance of the Australian Privacy Commissioner in relation to the Code states that:

> An impact on the privacy of individuals will be 'significant' if the consequences of the impact are considerable, taking into account their nature and severity.
> The consequences of a privacy impact could be significant for one individual or a group of individuals, for example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. The consequences of the potential privacy impacts for a group of individuals may vary based on their individual circumstances, so you should consider whether some individuals may be more significantly impacted than others.
> Sometimes projects can have a significant collective impact on society, rather than impacting on people individually. These collective impacts are likely to lead to broad public concern, for example, increased surveillance and monitoring activities, or the establishment of sensitive personal information sharing arrangements between the Commonwealth and other entities.
> There is no definitive threshold to determine when an impact is 'significant' given each project will differ in nature, scope, context and purpose. Accordingly, agencies are advised to screen for factors that may raise a project's risk profile.[7]

Article 35 of the GDPR covers Data Protection Impact Assessments:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[8]

Some examples of circumstances in which European data privacy regulators expect a PIA to be conducted are:

- if you're using new technologies
- if you're tracking people's location or behaviour
- if you're systematically monitoring a publicly accessible place on a large scale
- if you're processing personal data related to "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[9]
- if your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects
- if you're processing children's data
- if the data you're processing could result in physical harm to the data subjects[10]

Although privacy impact assessments are becoming more common in relation to proposals for new applications and uses of personal information about individuals, there remains considerable disagreement as to:

- the threshold at which a privacy impact assessment should be undertaken (ie, what is a serious risk of harm to an individual?)
- the nature and range of "privacy harms" that should be assessed
- the criteria for assessment of risk and harm
- the level of potential risk of privacy harm and likely (or other) exposure to adverse impact at which a particular process or process should be assessed as requiring mitigation and
- the level of residual risk of harm which is permitted to remain after appropriate mitigation

Even where PIAs are conducted, as they are currently conducted in Australia, the outputs typically have a number of limitations:

- They are only commissioned upon project initiation, in relation to the project as then specified. They are therefore point of time and often not revisited and revised when a project pivots or is otherwise respecified or evolves.
- They focus upon a particular project and its inputs and outputs, and not outcomes upon individuals that may be affected in some way by use of outputs of the project. A process and practice may be adjudged as appropriately respectful of rights and legitimate expectations of individuals as to how personal information about them is handled, but the outputs of that process or practice then applied in an inappropriate way to affect outcomes which cause harm to individuals.
- They are often legalistic and formulistic, focussed upon whether a particular handling practice meets the formal requirements of privacy principles, rather than focussing upon the level of risks and harms of unexpected, unreasonable, unfair or otherwise harmful impacts upon individuals. Indeed, by framing a review as a "data privacy impact" assessment and not an assessment of risk of significant harmful effects upon individuals or society, significant adverse impacts that are outside that frame are often missed, ignored or underrated.
- They do not assess societal benefit against individual detriment, and accordingly do not bring a broader public policy or ethical frame to the evaluation of a particular project.
- They are conducted by "privacy officers" or lawyers rather than by multidisciplinary teams and

accordingly often do not bring into the review consideration of factors such as social responsibility, expectations of organisations, social licence, effect upon digital trust (ie in government and government agencies), reputational risk, ethics or other non-legal considerations.

It is sometimes suggested that "the problem with PIAs" can be addressed by reframing the factors assessed to include, for example, consideration of algorithmic bias, building transparency and accountability into machine learning, and application of project outputs to affect outcomes.

However, as should be apparent from the above, the problems cannot simply be addressed by adding more factors to an assessment process which has other flaws (as above summarised).

Another problem is that PIAs as commonly conducted in Australia often do not cause an effect to be given to emerging international best practice in mitigation of privacy risk through pseudonymisation and better technical data architecture and operational governance.

Many PIAs are drafted on the basis that information is either capable of being used to identify some individuals within a cohort data set (including through combination with other information, or with other data points that thereby facilitate mosaic re-identification) and therefore (binary) either regulated as personal information about individuals, or not regulated as personal information about individuals.

By contrast, the GDPR addresses information purportedly de-identified by removal of direct identifiers (ie name and address of the individual to whom a transaction statement relates), as personal data that is pseudonymised personal data (personal data that cannot be attributed to an individual without the use of additional information) and accordingly legally required to be handled in accordance with the GDPR.[11]

Pseudonymised personal data is required by the GDPR to be kept separately and subject to appropriate technical, operational, organisational and legal controls to ensure that re-identification of an individual is not possible. A contractor to a data controller may design and specify its data handling processing policies, processes, practices and procedures to ensure that the contractor complies with obligations of a "data processor" under the GDPR. The framework enables and creates incentives for good data governance, including through contractual protections consistent with appropriate technical, operational, organisational and legal controls being implemented by the data processor.

Revision of the Privacy Act should expressly address the role of data privacy management programmes and governance and assurance frameworks and processes to reduce risks in handling of personal information. PIAs have an important role to play, but only where they are well done. Today, many PIAs simply do not adequately address risks of substantial privacy harms to affected individuals.

## Compliance culture of many organisations (both businesses and government agencies) in relation to data privacy is poor

Many organisations do not empower privacy officers to participate in key decisions about design and specification of products and services, and instead seek to address privacy compliance as a documentation function.

A common exception from this shortcoming is the governance of information security. This exception illustrates the broader problem. In recent years most businesses and government agencies have significantly improved governance of information security, largely due to recognition that serious data breaches are likely to lead to loss of enterprise value, erosion of trust of persons that deal with the APP entity suffering a breach, and exposure to class actions and ransom claims. Exposure to regulatory penalties for serious data breaches may have been a factor in improving information security governance, but it is not the primary factor. Outside of management of information security, good data privacy practice has to date generally not been seen as a significant driver of enterprise value. As a result, many APP entities have a poor track record of implementation of data minimisation and data privacy by design and default, and in considering legitimate expectations of individuals in and to data privacy.

Fixing this problem requires rebalancing of incentives, regulatory requirements and sanctions to ensure that data privacy concerns that are not related to data exfiltration are accorded similar attention within APP entities to the attention now given to governance of information security.

Some APP entities will "move fast and break things" unless they consider that there is a significant risk of regulatory action and exposure to substantial penalties and sanctions for non-compliance with the statute. The Office of the Australian Information Commissioner (OAIC) is underfunded and under-resourced, particularly having regard to its increasing workload in relation to notifiable data breaches. Increases in penalties and sanctions will not change the compliance culture of many APP entities, unless the OAIC is also resourced:

- to be more actively involved in education and instruction
- to promote development of industry best practice

- to identify and call out examples of good privacy practices
- to investigate possible, less egregious breaches of the Privacy Act
- to run important but risky court cases
- to conduct sector benchmarking analyses and promote development of sector, product or service-specific standards and codes of practice and
- to conduct the kind of wideranging and open-ended policy and industry reviews that the ACCC is funded to undertake

The right of individuals to data privacy has been accorded a lesser status than the right of consumers not to be misled. Each right is important. Individuals should be afforded protection of legitimate expectations of data privacy even when they are not consumers.

Fixing this problem requires commitment by the federal government to fund and staff the OAIC so that the OAIC is able to properly do its job.

It is unfair and unrealistic to expect the OAIC to be an active and effective regulator with its current constraints in funding and resourcing.

## Conclusion

We need to go back to basics.

Regulation of data privacy generally, and specifically of collection, use and sharing of geolocating and other individuating data collected from use of smartphones, IoT devices, digital search and social media platforms, content platforms, product and service comparison and ecommerce sites, is essential to enable citizens to go about their lives with reasonable seclusion.

Privacy law is now an important element in the framework of digital trust required to enable citizens to work, play and otherwise participate in their communities (however they choose to define them), in Australian society, and in the global economy.

Privacy law reform should:

- protect legitimate interests and rights of individuals in and to data privacy (regardless of whether those individuals are consumers) and
- nurture digital trust of citizens, to the benefit of affected citizens and of broader communities and societal interests but also
- reasonably accommodate the imperative for governments agencies and businesses to derive efficiencies of operation and provide citizens with benefits derived from data and technology-driven innovation

As with the government data-sharing reforms proposed by the federal government,[12] citizens and agencies need to be empowered to understand why and how reasonable and proportionate collections and handling of personal information about individuals can deliver efficiencies and benefits while not undermining their digital trust and their rights to and interests in data privacy.

Data privacy is not just a consumer protection issue. Among other reasons, the relevant collection and handling of data may or may not be associated with a consumer transaction. Rights and interests of citizens in relation to data about the need to be protected regardless of whether they are engaged in a consumer transaction. Protection of legitimate rights and interests of individuals in and to data privacy should not be principally addressed through consumer protection regulation.[13]

This Review provides an opportunity for the federal government to propose, and the Australian Parliament to legislate, a framework of privacy risk assessment, risk management and governance and assurance processes and practices that APP entities should adopt to demonstrate accountability, as well as transparency, as to their collection and handling of personal information. That opportunity is rarely presented to our legislature. Many Australian citizens should be interested in seeing that this opportunity does not go to waste.

***Peter Leonard***
*Principal, Data Synergies Pty Limited*
*Professor of Practice, UNSW Business School*
*Consultant, Gilbert + Tobin Lawyers*
*pleonard@datasynergies.com.au*

***About the author***

*Peter Leonard is a data and AI business consultant and lawyer advising businesses and government agencies. Peter chairs the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards, including the statutory NSW Information and Privacy Advisory Committee, which provides ongoing strategic advice to NSW Government as to data privacy.*

## Footnotes

1. As "transparent" is used in Australian Consumer Law, s 24.
2. Parliament of Canada, House of Commons of Canada: Bill C-11, 17 November 2020, https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.
3. Above, cl 11.
4. See further Office of the Australian Information Commissioner (OAIC), Guide to undertaking privacy impact assessment, 4 May 2020, www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/;

Information and Privacy Commission, Guide to Privacy Impact Assessments in NSW, May 2020, www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw; Office of the Victorian Information Commissioner, Privacy Impact Assessment, https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/; Office of the Information Commissioner Queensland, Undertaking a Privacy Impact Assessment, 25 July 2018, www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment.

5. OAIC, When do agencies need to conduct a privacy impact assessment?, 14 September 2020, www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/.
6. Above.
7. Above n 6.
8. GDPR.EU, General Data Protection Regulation (GDPR), https://gdpr.eu/article-35-impact-assessment/.
9. *Regulation (Eu) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* L119/1.
10. European Commission, Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) adopted by the European Data Protection Board, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236; https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_en.
11. Intersoft Consulting, General Data Protection Regulation, Arts 2(1), 4(1); Regulation (EU) 2016/679 of the European Parliament and of the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council, Recitals 15, 26 and 30 https://gdpr-info.eu/.
12. The Data Availability and Transparency Bill 2020 (Cth) currently before the Federal Parliament.
13. See further K Manwaring "Will Emerging Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation" (2018) 26(2) *Competition and Consumer Law Journal* 141; K Manwaring "Emerging Information Technologies: Challenges for Consumers" (2017) 17(2) *Oxford University Commonwealth Law Journal* https://ssrn.com/abstract=2958514.

**For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047**
**Cite this issue as (2021) 18(2) *PRIVLB***
**SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au**
**SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067**
**CUSTOMER RELATIONS: 1800 772 772**
**GENERAL ENQUIRIES: (02) 9422 2222**
**ISSN 1449-8227 Print Post Approved PP 243459/00067**