gadens

Privacy Act Review
October 2020

Submission from Gadens

29 November 2020

Introduction

Gadens is pleased to have the opportunity to make a submission in response to the questions raised in the Privacy Act Review (Issues Paper – October 2020) (**Issues Paper**).

We have focussed our submission on several of the key areas identified in the Issues Paper and would like to thank those Gadens' clients who responded to our privacy survey and also separately contributed to the submission. Our submission sets out our comments and observations regarding the areas of the Issues Paper that we consider will have the most significant impact on individuals and/or will raise important commercial or legal compliance issues.

Any defined terms used in our submission have the meaning given in our submission or are otherwise defined in the Issues Paper.

We look forward to contributing the next issues paper to be released early in 2021.

The small business exemption

1. Shifting community attitudes

(a) In September 2020, the Office of the Australian Information Commission (**OAIC**) conducted a survey to gauge the Australian community's attitudes to privacy. The results of the survey were telling and reinforced the importance of privacy to Australians with 70% of those surveyed describing personal information as "…an important issue and a major concern in their life."[1]

(b) Although extensive, the survey did not consider the small business exception in much detail highlighting that its operation has been somewhat neglected and that the Act has failed to keep up with the rapid advancement of technology.

(c) This however is problematic and is no longer in line with community values as the biggest perceived privacy risk in 2020 according to the OAIC's Australian Community Attitudes to Privacy Survey was identity theft and identity fraud.[2]

(d) This is a well-founded cause for concern as many small businesses deal with information relating to an individual's identity and are more susceptible to being compromised from a technological perspective by virtue of their relatively low levels of security.

2. The three million dollar question

2.1 Issue for comment

Is the current threshold appropriately pitched or should the definition of small business be amended? If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as number of employees or value of assets or should the definition be amended in another way?

1 Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey* (Survey, September 2020) 17.

2 Ibid 4.

2.2 Gadens comment

(a) The small business exemption was introduced approximately two decades ago which raises questions as to its currency, adequacy and relevance in a society which has seen significant strides with regards to technological advancement and its attitude towards same.

(b) 40% of respondents to our survey indicated that the current financial threshold of $3 million is too high and should be amended.

(c) In July 2019, the Australia Small Business and Family Enterprise published its "Small Business Counts" report which determined that approximately 93% of small businesses had an annual turnover of less than $2 million in 2017 to 2018.[3]

(d) These results have been extracted from the report and can be found below.

(e) Based on these figures, over two million of small businesses in Australia are not captured by the APPs by virtue of their annual turnover (unless the relevant exceptions apply).

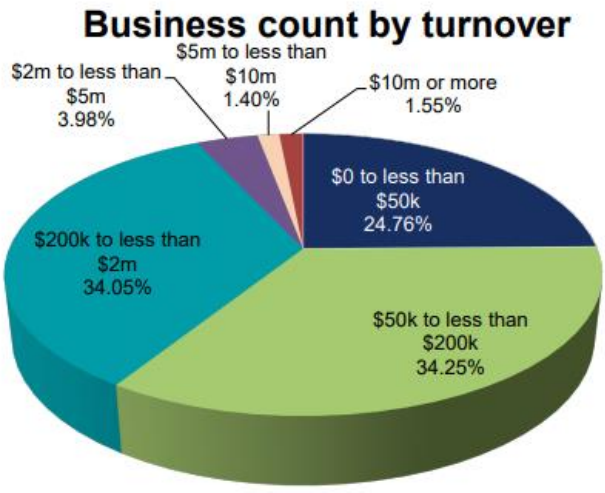
(f) If a financial threshold is to remain in place to determine the ambit of the small business exception, we submit that the threshold should be substantially reduced from the current $3 million threshold.

Table 2: Business numbers by annual turnover in 2017-18

Turnover	No. of businesses	%
$0 to less than $50k	572,826	24.76%
$50k to less than $200k	792,373	34.25%
$200k to less than $2m	787,685	34.05%
$2m to less than $5m	92,126	3.98%
$5m to less than $10m	32,483	1.40%
$10m or more	35,798	1.55%
Total	2,313,291	100.00%

Source: ABS Counts of Australian Business 8165.0, Table 17, Feb 2019 and ASBFEO calculations (excludes nano businesses with no GST role)

Chart 2: Business count by turnover



Source: ABS Counts of Australian Business 8165.0, Feb 2019 and ASBFEO calculations (excludes nano businesses with no GST role)

[3] Australian Small Business and Family Enterprise Ombudsman, *Small Business Counts: Small business in the Australian economy* (Report, July 2019) 8.

3. Where to from here? A realistic and practical balancing act

3.1 Issue for comment

> Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?

3.1 Gadens comment

(a) Proponents for the small business exemption maintain that its current form strikes the right balance between protecting the privacy rights of individuals whilst avoiding the imposition of unnecessary compliance costs on small business.

(b) Despite this, we are of the view that the:

  (i) law has fallen far behind the rapid advancement of technology;

  (ii) law has not adequately responded to changing societal attitudes when considered from a domestic and international perspective; and

  (iii) small business exemption is no longer fit for purpose.

(c) In support of this proposition, 79% of respondents to our survey indicated that small businesses pose significant risks to the privacy of individuals and that law has fallen far behind the rapid advancement of technology.

(d) According to a 2019 report prepared by 4iQ, there was a 424% increase in new data breaches and leaks of small business globally during the year of 2018 when compared to the year of 2017.[4]

(e) In Australia, NortonLifeLock found that one in four small businesses were subject to cybercrime in 2017 (up from one in five small businesses in the previous year).[5]

(f) We submit that there are significant gaps within the Act which must be addressed as it is clear that the amendments introduced 20 years ago did not and could not adequately consider the challenges and risks associated with technology, and in particular, the ever-expansive nature of the internet and its effects on small business.

(g) Although challenging, there are potential methods of balancing the privacy rights of individuals and imposing reasonable obligations and penalties upon small businesses for a breach of the Act.

(h) Rather than a blanket exemption, this may include the introduction of civil penalties that are more aligned to the general size and means of small businesses in Australia. This may include civil penalties which are imposed:

  (i) on a reduced rate, if a business comes within the small business threshold; or

  (ii) in line with the Act's penalty units as it relates to breaches caused by individuals.

(i) The imposition of either method of enforcement would reiterate the importance of privacy to Australians and protect their information at a greater scale whilst ensuring that small businesses are not penalised on the same basis as large and multi-national corporations.

(j) One potential method of assisting small businesses in complying with the Act could be to offer government grants or providing them with pro-forma documents to assist with compliance in a relatively simplified manner.

(k) We submit that the amendment of the small business exemption to allow for APPs to fully apply to most, if not all, small businesses would allow for:

  (i) greater accountability and community confidence;

  (ii) increased safety as it relates to an individual's information; and

4 4iQ, *Identity Breach Report 2019 "Identities in the Wild: The Long Tail of Small Breaches"* (Report, February 2019) 6.

5 NortonLifeLock, *Norton SMB Cyber Security Survey: Australia 2017* (Survey, 2017) 3.

(iii) greater consistency with other jurisdictions which in turn will reduce one of the key outstanding issues preventing Australia from achieving adequacy with the EU.

Employee Records Exemption

4. Scope of the employee records exemption

4.1 Issue for comment

Is the personal information of employees adequately protected by the current scope of the employee records exemption? Should some but not all of the APPs apply to employee records, or certain types of employee records?

We are of the view that:

(a) The current scope of the employee records exemption needs to be clarified.

(b) Subject to clarification of what would constitute genuine consent from an employee, the scope of the employee records exemption should be adjusted so that certain types of sensitive information would be subject to the protections of the Act.

(c) Sensitive information that would be subject to the protections of the Act could include health information about an individual or genetic information about an individual that is not otherwise health information.

4.2 Overview of existing regulatory framework

(a) The exemption applies to an organisation acting in its capacity as employer or former employer of an individual in relation to acts or practices that are directly related to the employment relationship.[6]

(b) The exemption does not cover prospective employees that are subsequently unsuccessful.[7]

(c) The exemption covers any record of personal information relating to an employee,[8] including the terms and conditions of employment of an employee, or the engagement, training, disciplining, resignation or termination of employment of an employee.

4.3 Gadens comment

(a) In light of the recent decision by the Full Bench of the Fair Work Commission,[9] it is currently unclear whether the employee records exemption applies to the act of collecting personal information from employees:

(i) If the APPs apply up to the point an employee record is generated, then the Act should be amended to clarify which specific APPs organisations will need to comply with, such as APP 3 and APP 5, to give organisations clarity on their compliance requirements.

---

[6] *Privacy Act 1988* (Cth), section 7B(3).

[7] Office of the Australian Information Commissioner, *Employee Records Exemption* (Web Page) <https://www.oaic.gov.au/privacy/privacy-for-organisations/employee-records-exemption/>.

[8] *Privacy Act 1988* (Cth), section 6(1).

[9] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.

(ii) However, the practicality of this position should be considered further. During the course of an employment relationship, there will be various points of collection of an employee's personal information, some of which may be trivial or repetitive.

(iii) From the organisation's perspective, it may be impractical or cause undue burden to comply with APP 3 and APP 5 at each point of collection, no matter how trivial. From an individual's perspective, there is a risk of information overload and consent fatigue.

(b) It may be more reasonable to adjust the scope of the employee records exemption so that certain APPs apply to certain stages of an employment relationship. For example, it would be reasonable to expect that APP 3 and APP 5 will apply at the start of an employment relationship.

(c) Further, it may also be more reasonable to adjust the scope of the employee records exemption so that certain APPs apply to certain types of personal information such as sensitive information. However:

(i) A growing number of organisations are implementing the use of biometric verification or authentication as part of their physical security controls. We think that it is likely that these forms of technology will continue to be taken up by organisations over time.

(ii) Individuals are growing more and more comfortable with using biometrics as a means to verify and authenticate access. Smart phone developers and companies have introduced the use of biometric verification or authentication in everyday devices through the use of technologies like Touch ID and Face ID.

(iii) Organisations may have a reasonable and genuine reason for using certain types of sensitive information, such as biometric templates. We think that these types of sensitive information should fall within the scope of the employee records exemption, noting that:

(A) it is unclear whether an employee could give genuine consent to the collection of their sensitive information; and

(B) organisations may experience undue compliance burden. For example, an organisation may be required to maintain two physical security systems if one employee does not consent to the use of their biometric information for the purpose of verification or authentication.

(d) Nonetheless, we think there is a view within organisations that certain types of sensitive information should be protected under the Act. Our survey indicates that 80% of our survey participants are favourable to the protection of certain types of sensitive information falling outside of the scope of the employee records exemption.[10]

(e) In our view, health information about an employee or genetic information about an employee that is not otherwise health information should be protected under the Act. These types of sensitive information are usually collected for the purpose of accommodating an employee's health conditions, and we consider that these types of sensitive information would not otherwise be used by an organisation in its operations generally.

[10] Gadens, *Privacy Act Review – Gadens Survey* (November 2020).

5. Employees' consent

5.1 Issue for comment

If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

We are of the view that the Act should clarifying what vitiating factors will apply that will call an employee's consent into question.

5.1 Overview of existing regulatory framework

(a) Consent means express or implied consent.[11]

(b) Consent must be adequately informed, given voluntarily, and current and specific.[12]

5.2 Gadens comment

(a) We think it is reasonable that the threat of disciplinary action or dismissal should be considered to be a vitiating factor in assessing whether an employee's consent is genuine or not.[13] However, such a change should be coupled with the clarification discussed in section 4.3 of our submissions to strike an appropriate balance between protecting employees' sensitive information and the compliance burden on organisations.

(b) We do not agree that the employee records exemption should be removed in its entirety. We note that 47% of our survey participants indicated that the removal of the employee records exemption would make it difficult for their respective organisations to comply with the Act.[14]

Consent to collection, use and disclosure of personal information

6. Use of personal information for direct marketing

6.1 Issue for comment

Does the Act strike the right balance regarding the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

For the reasons detailed below, we are of the view that:

(a) by and large, the current regulatory framework appropriately balances the rights of individuals and businesses in relation to the use of personal information for direct marketing;

(b) some further harmonisation and clarification as between APP 7, the Spam Act and the DNCR Act would be desirable; and

(c) there would be limited practicality or benefit in introducing additional precautions for individuals and such precautions would instead likely result in:

(i) increased consent fatigue for individuals; and

[11] *Privacy Act 1988* (Cth), section 6(1).

[12] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines, Chapter B: Key Concepts* (Web Page) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/>.

[13] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946, [58].

[14] Gadens, *Privacy Act Review – Gadens Survey* (November 2020).

(ii) unnecessary compliance burdens for businesses.

6.2 Overview of existing regulatory framework

(a) Under the APPs, "direct marketing" involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. [15]

(b) The APPs set out specific circumstances where personal information can be used for direct marketing. It is not generally necessary that an individual consents to receive direct marketing, unless the direct marketing is by email or SMS (and therefore falls under the Spam Act).[16]

(c) Direct marketing may be permissible if the individual would reasonably expect to receive direct marketing or if (in some cases) the individual would not have that expectation but is given a prominent statement about how to opt out.

(d) However, under both scenarios, there must be a method for the individual to opt out of receiving the direct marketing. [17]

(e) APP 7 does not apply to the extent that the Spam Act or the DNCR Act apply.[18]

6.3 Gadens comment

We are of the view that the status quo should largely be maintained in relation to direct marketing under the Act and the APPs.

Opt out

(a) Firstly, the APPs currently already require businesses to provide individuals with a 'simple means' to opt out of receiving direct marketing. [19]

(b) If an individual does not want to receive direct marketing from a business, they can elect to 'opt out' and not receive such communications.

(c) This process is required under the APPs and the OAIC's guidance to be free, straightforward, prominent and easily accessible. We are of the view that this is generally working reasonably well in the marketplace.

Reasonable expectation

(d) Currently, personal information that has been collected directly from an individual can be used for direct marketing where the individual would reasonably expect their personal information to be used for the purpose of direct marketing.

(e) The 'reasonably expect' test is objective. Important factors for this test can include whether:

(i) the individual has consented to the use or disclosure of their personal information for that purpose;

(ii) the organisation has notified the individual that one of the purposes for which it collects the personal information is for the purpose of direct marketing; and

(iii) the organisation made the individual aware that they could request not to receive direct marketing communications from the organisation, and the individual has not made such a request. [20]

(f) The above should provide individuals with sufficient information regarding the use of their personal information prior to the business being able to use the personal information for direct marketing.

Consent under the Spam Act

(g) In the current digital age, individuals receive the majority of their direct marketing via SMS or email and the Spam Act already provides additional consent requirements in these circumstances.

(h) Under the Spam Act:

---

[15] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 81.

[16] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) Chapter 7.

[17] Ibid.

[18] APP 7.8.

[19] *Australian Privacy Principles Guidelines* at 7.27 - 7.30.

[20] Ibid at 7.15.

(i) an individual is required to provide express consent to receive marketing emails or text messages (or in some circumstances consent can be inferred); and

(ii) an opt out option must be available.

(i) We do not believe there is any evidence of a need to amend the APPs to require that individuals consent to receive direct marketing materials (such as "snail mail" direct marketing).

(j) However we do think that the fact that different forms of direct marketing are governed by different pieces of legislation (see APP 7.8) is confusing.

(k) Further, the precise meaning of APP 7.8 is debatable – for example, if the Spam Act applies to an instance of direct marketing (because it occurs via email), does that mean that none of APP 7 applies to that communication? For example, would consent be required in order to use sensitive information for that direct marketing (see APP 7.4)? We submit that there is scope to clarify APP 7.8.

Informed consent

(l) We understand that the DPI Report found that it is often difficult for individuals to understand how their personal information is being used as businesses induce consumer consents to data collection and use (including direct marketing) by relying on long and complex contracts, or all or nothing click wrap consents which may prevent individuals from making informed decisions. [21]

(m) We submit that the existing concepts of "consent" and "reasonable expectations" already cater to this situation. For example, query if a consent in such a scenario would be legally effective if it is bundled with various other purposes – see the discussion of "consent" in the OAIC's guidelines on the APPs.

7. Consent and pro-consumer defaults

7.1 Issue for comment

The questions we have considered are whether:

(a) entities collecting, using and disclosing personal information should be required to implement pro-privacy defaults for uses and disclosures of personal information; and

(b) individuals should be required to separately consent to each purpose for which an entity collects, uses and discloses information. What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

Notably:

- The DPI report recommended that entities should only collect information needed to provide their products or services and that settings enabling data processing for a purpose other than the performance of a contract should be pre-selected to be 'off'.[22]
- Under that recommendation, any consent for a particular purpose would need to be de-bundled from other purposes and separate consents provided. [23]

While we fully acknowledge the need for consumers to be informed about the use of their personal information, we are of the view that it is not necessary that:

(c) individuals be required to provide a separate consent for each purpose; or

(d) defaults relating to the use of personal information for secondary purposes always be pre-selected to "off".

7.2 Overview of existing regulatory framework

(a) The APPs currently require individuals to provide consent when their personal information is collected in limited circumstances. Under APP 6, consumers are not required to provide consent when their personal information is used or disclosed for a 'primary purpose'. [24]

[21] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report*, 26.

[22] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report*, 464 – 470.

[23] Ibid.

[24] Privacy Act (n 16) sch 1, cl 6.

(b) The OAIC currently already endorses a relatively narrow approach to the interpretation of the concept of 'primary purpose'.

7.3 Gadens comment

Separate consent

(a) We are of the view that creating separate consent requirements for each purpose for which an entity collects, uses and discloses information will likely create an overload for consumers (resulting in consumer confusion and consent fatigue) and create extensive administrative and regulatory burdens for businesses and agencies.

(b) Whilst theoretically requiring individuals to consent to each purpose for which an entity collects, uses and discloses information would allow the individual to be informed, this information:

(i) is already required to be included in APP entities' privacy collection statements and (in less specific detail) their privacy policies; and

(ii) will likely result in individuals simply ignoring a proliferation of consent requests, or perhaps ticking more boxes without actually reading the information provided as they will want to receive the associated good or service.

(c) It should not be assumed that imposing additional privacy compliance requirements on businesses and agencies will necessarily be in the best interests of consumers. Consumers have an interest in entities having the freedom (within the constraints of existing laws) to use personal information in innovative ways, without being unduly constrained by having to obtain a separate consent for each collection, use or disclosure – innovation and competition in these areas will in many cases benefit the consumer. An overly prescriptive privacy law regime risks stifling growth and innovation amongst data-focussed businesses and imposing costs that will ultimately be passed on to consumers.

Pro-consumer defaults

(d) Whilst pro-consumer defaults might in theory encourage individuals to be confident about how they engage with an entity, we do not consider that pre-selected 'off' data settings will necessarily 'best' allow individuals to protect their personal information. Combined with any new requirements around consent and disclosure not being bundled, this would effectively see consumers having to check a box for each act of data processing, providing a huge burden for individuals.[25]

(e) Seeking "opt in" consent for every type of act of data processing undertaken by a business would result in consumer fatigue and result in increased compliance and operational costs for businesses. Moreover, consumers will also miss the benefits of opt-out consents as a result of these changes. For example, individuals benefit from receiving advertising targeted to the individual or updates regarding sales.

(f) Our experience is that in many situations, a consumer can be automatically "opted in" to secondary purposes through clear communication to them that this will occur (for example, through a prominently presented pre-ticked box that the individual may elect to un-tick, or simply through prominent and clear wording that explains the secondary purposes). The key is clear, transparent communication by the entity to the individual. In our experience this approach, when properly implemented, does not generate any material number of complaints or concerns by the individuals.

(g) The mooted changes would result in increasingly complex and burdensome tasks for consumers in the digital economy and potentially make the consents sought by businesses longer, more complicated and more difficult for consumers to understand.

(h) Whatever position the law takes regarding consent, it would be helpful if the OAIC could provide guidance to businesses and agencies in the form of templates or "good practice examples" for gaining consent and for related purposes such as giving a privacy collection statement. This could also help consumers as they will gradually become more readily able to spot conduct in the marketplace that does

[25] Indue, Submission to the ACCC Digital Platforms Inquiry, January 2019; Nine, Submission to the ACCC Digital Platforms Inquiry, February 2019; Facebook, Submission to the ACCC Digital Platforms Inquiry, March 2019.

not follow the usual template or "good practice" and consider the situation more carefully before proceeding.

8. Withdrawal of consent

8.1 Issue for comment

Should entities be required to expressly provide individuals with the option of withdrawing consent?

8.2 Overview of existing regulatory framework

(a) The Act does not explicitly provide individuals with the right to withdraw consent.

(b) However, the APP Guidelines state that an individual may withdraw their consent and this should be an easy and accessible process.[26]

(c) The approach under the APP Guidelines is consistent with the position under the GDPR, being that the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Before giving consent, the data subject must also be informed about his or her right to withdraw consent anytime.[27]

8.3 Gadens comment

(a) We are of the view that individuals should be provided with the opportunity to withdraw their consent (as already provided under the APP Guidelines) and should be informed of this right (as is the position under the GDPR). However, businesses should not be required to provide ongoing reminders to individuals about their right to withdraw consent.

(b) Based on our experience, in practice, if a business receives a request from an individual to withdraw consent to a use of their personal information, the business will use all reasonable endeavours to comply with this request (in accordance with the APP Guidelines).

(c) Whilst there is an argument that individuals have a limited opportunity to reconsider their initial consent, we consider that individuals are not more likely to reconsider their initial consent if they are given the option to withdraw it.[28] Rather, they will quickly become jaded under an onslaught of messages prompting them to consider whether they wish to withdraw their consent to various things. We expect that "reminder fatigue" would soon set in and individuals would for the most part learn to ignore these messages.

(d) If individuals are informed at the time of giving their initial consent, they will be aware of this right and can make a decision at any point to withdraw their consent. This is much less likely to result in fatigue by individuals and would avoid imposing unnecessary compliance costs on businesses and agencies.

9. Definitions

Meaning	Abbreviation
Australian Competition and Consumer Commission	ACCC
Australian Privacy Principles	APPs
Do Not Call Register Act 2006	DNCR Act
General Data Protection Regulation	GDPR
Spam Act 2003 (Cth)	Spam Act

[26] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) B.48-B.51.

[27] General Data Protection Regulation, Article 7.

[28] Privacy Act Review (Issue Paper – October 2020), 46 – 47.

Overseas data flows and third party certification

10. Overseas data flows

10.1 Issue for comment

What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?

10.2 Gadens comment

(a) The accountability approach ensures that APP entities who disclose personal information to overseas recipients carefully consider whether, how, and to whom they disclose information.

(b) On one hand, the fact that an APP entity is accountable for acts or practices of an overseas recipient encourages good privacy practices. Before disclosure APP entities are required to consider the privacy obligations of the recipient and whether the recipient is likely to handle the information in an appropriate way.

(c) On the other hand, the consideration of the recipients' privacy obligations may have a stifling effect on the flow on information. APP entities may be reluctant to transfer data overseas, even where they have robust contractual provisions in place with the recipient, as they are accountable for actions or practices that are out of their control.

10.3 Exception – overseas recipient subject to law or scheme substantially similar to APPs

(a) To enjoy the "substantially similar" exception in APP 8.2 an APP entity must properly consider both the APPs and the privacy law or scheme in the recipients' country.

(b) This consideration is generally based on legal or privacy advice. The process of requesting and considering such advice ensures that an APP entity actively considers the information they are seeking to disclose, the APPs, and the foreign privacy scheme. This is a positive outcome and ensures privacy is central when an APP entity considers disclosing personal information overseas.

(c) However, the requirement to compare the APPs and a foreign privacy scheme can create a significant barrier to the flow of information. Seeking advice, particularly in relation to a foreign jurisdiction, can be difficult and expensive for many businesses.

(d) An official list which indicates which countries the Australian Government considers to have substantially similar privacy schemes to the APPs would greatly assist businesses, save time and money, and enable them to confidently rely on the exception in APP 8.2.

(e) This view is supported by Gadens' clients. 93% of respondents answered yes to the question: "would you rely on an Australian Government official list, indicating overseas countries with privacy schemes substantially similar to the APPs, if disclosing personal information overseas?" 7% of respondents stated they were unsure.

10.4 Issue for comment

Are APP 8 and section 16C still appropriately framed?

10.5 Gadens comment

(a) Section 16C could be clarified to make clear that it only applies to disclosures of data overseas, and that this does not capture transfers that are not 'disclosures'.

10.6 Issue for comment

Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?

10.7 Gadens comment

(a) Yes, as the removal of the exemption would likely create commercial tensions for multinational companies. For example, where a company was required to carry out an action in another jurisdiction in compliance with that jurisdictions law, and that action was in breach the APPs. A company may be in a position where they have to consider which law they should not comply with.

(b) To avoid finding themselves in such a position, companies may curtail the flow of data to reduce the risk that they were required to carry out an action contrary to the APPs. The exception provides a necessary high bar that must be cleared before a person can contravene the APPs and encourages the flow of data.

10.8 Issue for comment

What (if any) are the challenges of implementing the CBPR system in Australia?

10.9 Gadens comment

(a) It may be difficult to receive 'buy in' from Australian businesses to implement or participate in the CBPR system in Australia. The prospect of adhering to a further privacy scheme may be viewed as overly burdensome.

(b) Some businesses may consider that the APPs and the CBPR (and the GDPR if they adhere to it) are all for the same purpose, or all achieve the same result. For smaller businesses in particular, the CBPR may be considered an unnecessary duplication and viewed as being too resource intensive.

(c) The certification process, and the annual charge for certification and ongoing compliance costs may serve as disincentives for businesses to participate.

10.10 Issue for comment

What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

10.11 Gadens comment

(a) A voluntary domestic privacy certification scheme could include a certification logo. Companies could display the logo on their website or products to indicate to consumers that they comply with the domestic certification scheme.

(b) The certification logo could be similar to the Heart Foundation "tick" or the made in Australia logo. The logo may provide a competitive advantage to companies, as consumers would understand that companies which displayed the logo have been certified as adopting good privacy practices.

(c) Additionally, the scheme may incentivise businesses to seek certification in order to display the certification logo, which in turn may lift the standard of privacy compliance in Australia.

10.12 Issue for comment

What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

10.13 Gadens comment

(a) We note the issues paper highlights that the APEC region is a more significant trading partner than the EU and that as a result the Government's recent priority has been to ensure adequacy with APEC economies.

(b) Our experience is that the GDPR is considered the benchmark privacy scheme. The fact that the APPs are not considered adequate under the GDPR causes significant, well understood, issues for Australian businesses seeking to engage with European business or customers, and can act as a deterrent for doing so.

(c) The clear Advantage of GDPR adequacy would be that companies wishing to disclose or receive information to companies governed by the GDPR would not have to enter into additional contracts due to the APPs not being considered adequate. This may result in reduced expenses for business in not having to engage lawyers to draft additional privacy provisions into contracts.

(d) A significant disadvantage of achieving GDPR adequacy is that it would place greater impositions on Australian businesses. In particular small businesses who may be brought into the operation of the Privacy Act. Small businesses may be less likely to benefit from the Privacy Act being adequate under the GDPR as they may be less likely to transfer data overseas.

(e) 93% of respondents to our survey stated that the Privacy Act should be reformed so that it provides an adequate level of data protection for GDPR. 7% of respondents states they were unsure.

(f) However, the survey may not have captured small businesses who have not previously required privacy advice or other commercial legal advice. If such businesses were included in the survey, the results may differ, as small businesses may not be enthused about being brought into the purview of the Privacy Act which would likely be necessary to achieve GDPR adequacy

Notifiable Data Breaches Scheme

11. Changes to entities' practices

11.1 Issue for comment

Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme? Has the NDB Scheme raised awareness about the importance of effective data security?

We are of the view that the NDB Scheme has been effective in raising awareness about the importance of effective data security, particularly around the importance of supplier arrangements.

11.2 Overview of existing regulatory framework

(a) An organisation's obligation to notify the Commissioner and affected individuals is triggered if the organisation becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach or that there has been an eligible data breach.[29]

(b) Where an organisation suspects that there has been an eligible data breach, it has 30 days to make an assessment as to whether one had in fact occurred.[30]

11.3 Gadens comment

(a) Since the introduction of the NDB Scheme, organisations have scrutinised their supplier arrangements in more detail. This has largely involved the review of supplier arrangements and putting in place appropriate contractual measures to ensure that a supplier would provide the assistance and information that an organisation would reasonably require in order to comply with the Act should an eligible data breach originate from the supplier.

(b) However, there is complexity involved in the use of certain suppliers, such as those providing cloud service products. For example:

(i) Some cloud service products require a technology stack in order to function. A technology stack are the other products needed in order to run a single application.

[29] *Privacy Act 1988* (Cth), section 26WH and section 26WK.

[30] *Privacy Act 1988* (Cth), section 26WH(2).

(ii) Notwithstanding this, an organisation would only have a contract with the supplier providing the application.

(iii) Should an eligible data breach originate in one of those other products in the technology stack, the organisation has limited ability to compel that third party to provide assistance or information.

(c) To address the complexity around multi-party breaches, we think that the NDB Scheme should be amended to include express obligations on a supplier to provide assistance to organisations affected by an eligible data breach originating from the supplier. This view is supported by 87% of our survey participants.[31]

(d) Notwithstanding the above, the impact of such a change on suppliers should also be considered. This may be addressed by specifying what assistance or information would be required from a supplier in a limited, exhaustive manner. It should also be made clear that the organisation will ultimately be responsible for complying with its obligations under the NDB Scheme.

12. Compliance across multiple frameworks

12.1 Issue for comment

Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

We are of the view that the alignment of the NDB Scheme with other international frameworks and domestic frameworks should be considered.

12.2 Overview of existing regulatory framework

The NDB Scheme does not address circumstances where there is an overlap with other domestic and international frameworks.

12.3 Gadens comment

(a) Around 60% of our survey participants have experienced significant difficulties in complying with multiple international frameworks alongside the NDB Scheme.[32] We think that this is of particular concern for small to medium enterprises that are looking to expand their reach to overseas markets but still maintain a single operating entity in Australia.

(b) In addition to the above, other organisations may also be subject to domestic frameworks such as those set out in APRA Prudential Standard CPS 234.[33] Unfortunately, these domestic frameworks may not be aligned with the Act.

(c) We think that there should be a level of flexibility where multiple domestic or international frameworks apply, and the Act should be amended to take this into account in light of the time limitations applicable to assessing whether an eligible data breach has occurred.

[31] Gadens, *Privacy Act Review – Gadens Survey* (November 2020).

[32] Gadens, *Privacy Act Review – Gadens Survey* (November 2020).

[33] Australian Prudential Regulation Authority, *Banking, Insurance, Life Insurance, Health Insurance, and Superannuation (Prudential Standard) Determination No. 1 of 2018* (CPS 234, 30 November 2018).

13. Concluding comments

Gadens welcomes the Government's decision to conduct a review of the Privacy Act. The DPI report highlighted the challenges of online platforms to traditional media as well as the evolving privacy issues for consumers seeking to access, use and benefit from technology in their everyday lives. The particular threats posed by cyber in this context and the growing awareness of the importance of privacy rights make now an opportune time to examine the current Privacy Act and those key elements which may require change.

Gadens thanks the Commonwealth Attorney General for the opportunity to comment on upcoming review of the Privacy Act. Please feel free to contact the authors listed below should you require further information or have any further queries.

Authors

Partners – David Smith, Hazel McDwyer and Dudley Kneller

Lawyers – Raisa Blanco, Lisa Haywood, Zein Jomaa and Gabe Abfalter