Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D20/20780

27 November 2020

Attorney General's Department

By email only: PrivacyActReview@ag.gov.au

Dear review team,

Submission in response to the Attorney-General's Department's Privacy Act Review Issues Paper

I am pleased to make a submission in response to the Attorney-General's Department's *Privacy Act Review Issues Paper* (**Issues Paper**).

My office, the Office of the Victorian Information Commissioner (**OVIC**) is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

I have organised my comments based on some of the key themes discussed in the Issues Paper. The key points in this submission are:

- The principles-based approach in the *Privacy Act 1988* (**Privacy Act**) provides a good framework for information governance and privacy best practice, as it offers privacy law the flexibility it needs to stay up to date with technological and other developments. However, to be effective, principles-based regulation must be overseen by an appropriately resourced regulator that is able to publish guidance, and in particular to take enforcement action. The Office of the Australian Information Commissioner (**OAIC**) regulates information management in a dynamic and large economy as well as an increasingly data-reliant government, and it should therefore be better resourced to enable it to carry out its functions and responsibilities in regulating a principles-based approach to privacy.

- In light of the significant increase in the amount of personal information collected, used and disclosed by political parties and small businesses, and changing community expectations, the exemption for these entities under the Privacy Act should be removed. This would bring the Privacy Act better in line with community expectations, by ensuring that individuals' privacy is better protected in circumstances where there is currently little to no privacy protection.

- There are challenges with the current consent model in the Privacy Act, particularly in relation to new technologies such as artificial intelligence (**AI**) and the Internet of Things (**IoT**), and community expectations of when their consent should be sought for the collection, use and disclosure of their personal information, and "consent fatigue" in which they are frequently bombarded by requests for data sharing they may not fully understand. Requirements to provide notices of collection could also be strengthened.

Definition of personal information

1. As discussed in the Issues Paper, the definition of personal information in the Privacy Act is intended to capture a broad range of information, and be sufficiently flexible and technology-neutral to cover changes in the way information that identifies individuals is collected and handled.[1] The definition of personal information, with only small modifications, has been largely effective in defining the coverage of the Privacy Act for the last 40 years.

2. OVIC acknowledges that technological advancements, data analytics developments and increases in the volume of technical data collected, used and shared in digital markets have influenced the types of information that could be considered as personal information. However, OVIC's concern is that updating the definition of personal information in the Privacy Act to include specific categories of information, such as location data, runs the risk of the definition becoming outdated as technology develops and community expectations about the kinds of information that should be protected change. Further, while in some cases information such as IP addresses and device identifiers may be able to reasonably identify an individual, this will not be true in all cases.

3. The Attorney-General's Department may wish to consider replacing the word 'about' with the phrase 'relating to' so that personal information is defined as 'information or an opinion *relating to* an identified individual, or an individual who is reasonably identifiable'. This alternative wording may align the Privacy Act more closely with international standards, such as those established by the General Data Protection Regulation (**GDPR**), while also potentially expanding the types of information subject to coverage by the Privacy Act to cover the sorts of information referred to in the Issues Paper.

4. OVIC recognises that updating the definition of personal information is likely to also result in compliance costs for entities regulated by the Privacy Act, as they would need to modify their systems and information handling practices. However, OVIC does not consider this a reason to delay making important changes to Australia's privacy law, where there is a perceived benefit to the community in doing so.

De-identified, anonymised and pseudonymised information

5. As noted in the Issues Paper, there are certain risks and challenges with using and disclosing de-identified data. De-identified data carries the inherent risk of re-identification when matched with other available data. There are also limits on the methods used to de-identify data and, particularly where unit-record level data is concerned, none of the methods can guarantee complete privacy.[2] Consideration should be given to implementing additional protections for de-identified, anonymised and pseudonymised data to minimise potential privacy risks.

6. It is important to highlight that while de-identified data is most often used for statistical and analytical purposes, it is also commonly used for micro-targeting; companies do not need to know the identity of an individual in order to target advertising towards them and will often exploit de-identified data – which is not considered to be personal information – to do so. Yet this does not change the privacy-invasive nature of micro-targeting practices. Much is often said about the negative impact of targeted political advertising on democracy, however targeted advertising as a whole is increasingly concerning. While it is argued that personalised adverts are beneficial for the consumer, they also have significantly harmful impacts on society and democracy. For instance,

[1] Issues Paper, p 16.
[2] See Office of the Victorian Information Commissioner, *Protecting unit-record level personal information*, May 2018, available at: https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf; Office of the Victorian Information Commissioner, *De-identification and privacy: Considerations for the Victorian public sector*, August 2018, available at: https://ovic.vic.gov.au/wp-content/uploads/2018/08/De-identification-Background-Paper-2018-Update-V1.pdf.

micro-targeting has normalised tracking and data mining, it drives surveillance capitalism and has led to the exponential growth of fake news.[3] The benefits may have been overstated, and the negative impacts almost certainly understated.[4]

7. OVIC is of the view that the negative effects of micro-targeting ought to be subject to stronger regulation. Possible ways in which this could be achieved include amending the definition of personal information to include information 'relating to' an individual, as discussed in point 3 above, and strengthening the protections for de-identified data so that its collection, use and disclosure is regulated, where it has the potential to infringe upon individuals' privacy.

Flexibility of the Australian Privacy Principles in regulating and protecting privacy

8. The Australian Privacy Principles (**APPs**), like the Information Privacy Principles (**IPPs**) in the PDP Act, generally provide a principles-based, flexible approach to protecting individuals' information privacy. As the Australian Law Reform Commission (**ALRC**) notes, principles-based regulation is designed to be technology-neutral, generally non-prescriptive and high-level so that it can apply to all entities subject to the Privacy Act, and also encompass the numerous ways in which personal information is handled in Australia.[5]

9. OVIC's experience administering the PDP Act has shown that the principles-based approach caters to the wide range of information handling practices that public sector organisations need to engage in to deliver public services in a privacy enhancing way. The flexibility afforded by the IPPs and APPs largely enables the principles to be adapted and applied over time to new technologies, initiatives and types of personal information.

10. While there are a number of mechanisms in the PDP Act that can allow public sector organisations to depart from the IPPs on approval of the Information Commissioner,[6] not many organisations have sought to rely on these mechanisms since they were introduced in 2014. OVIC has found that the IPPs have been sufficiently permissive and flexible to enable organisations to achieve their objectives while maintaining good privacy practices, demonstrating the effectiveness of a principles-based approach for privacy protection.

11. The APPs, combined with the legislative mechanisms to adapt the APPs under the Privacy Act, provide a good framework for balancing the protection of individuals' privacy with the interests of regulated entities in carrying out their functions and activities. Because principles-based rules are open to interpretation, it is necessary for the OAIC to be sufficiently resourced and given the necessary powers to apply the principles in a way that accords with community expectations, enforce adherence to the principles and provide appropriate guidance to regulated entities where needed.

Small business exemption

12. The Issues Paper explains that the small business exemption was introduced in the *Privacy Amendment (Private Sector) Act 2000* to minimise unreasonable compliance costs for small

[3] Arwa Mahdawi, 'Targeted ads are one of the world's most destructive trends. Here's why', *The Guardian* (online, 6 November 2019) available at https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy.
[4] Daniel Woods and Rainer Böhme, 'The Commodification of Consent, (Workshop on the Economics of Information Security, May 2020) available at https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final2.pdf.
[5] Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, 240, available at: https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf.
[6] See divisions 5 and 6 of the PDP Act for information on public interest determinations, temporary public interest determinations and information usage arrangements.

businesses, which posed little or no risk to the privacy of individuals. It has been 20 years since the exemption was introduced and, in that time, there has been a significant rise in the amount of personal information collected, used and disclosed by small businesses. This trend has been dramatically escalated by the increased emphasis on e-commerce and digital marketing. The volume of personal information held by many small businesses poses a high risk to privacy. In addition to being able to legally collect information about individuals without their knowledge or consent, many small businesses can, and do, use personal information for purposes that individuals are not aware of or would not reasonably expect.

13. The recent privacy concerns about the contact tracing practices of businesses provide a pertinent example.[7] In efforts to manage the spread of COVID-19, many businesses around Australia are now required to collect personal information from their patrons for contact tracing purposes. Some businesses are using digital check-in solutions provided by the private sector to collect personal information, while others are manually collecting the information from patrons using pen and paper. In both of these cases, there are concerns that the check-in data may be used for purposes other than contact tracing, in many cases without individuals' knowledge. There are also concerns around the adequacy of security measures implemented by businesses to ensure that check-in data is not lost, stolen or inappropriately accessed,[8] given the lack of regulatory oversight.

14. OVIC is of the view that small businesses should be subject to privacy regulation, as the risk to the privacy of individuals is undeniably higher now than it was two decades ago. Regulatory oversight would not only likely address the concerns arising from small businesses' contact tracing practices but would also ensure that the volume of personal information now held by many small businesses is appropriately protected. Further, Australia is the only jurisdiction among comparable jurisdictions such as New Zealand, Canada and the United Kingdom that exempts small businesses from privacy obligations.[9] Removing the exemption would align Australia with its global counterparts and give Australia a better chance at achieving adequacy with the European Union.[10]

15. Notably, the ALRC stated that 94% of Australian businesses are potentially excluded from the Privacy Act by the small business exemption.[11] Should this exemption be removed, it is crucial that the OAIC be provided significantly more resources to efficiently manage their increased regulatory responsibilities and deliver the necessary guidance to support businesses who have not previously had to comply with privacy law.

Employee records exemption

16. Employers often collect a range of personal information from their employees, including health information and criminal record information, and as the ALRC notes, there is a significant risk of harm to individuals if such information is used or disclosed inappropriately.[12] Under the PDP Act,

[7] Ellen Coulter, 'Businesses' collection of information for coronavirus contact tracing raises privacy concerns for customers', *ABC news* (online, 29 October 2020) available at https://www.abc.net.au/news/2020-10-28/information-privacy-small-business-coronavirus-contact-tracing/12821052.
[8] Kevin Nguyen, 'The QR code has turned COVID-19 check-ins into a golden opportunity for marketing and data companies', *ABC Investigations* (online, 2 November 2020) available at https://www.abc.net.au/news/2020-10-31/covid-19-check-in-data-using-qr-codes-raises-privacy-concerns/12823432; Jackson Worthington, 'Privacy expert concerned over digital check-in tools for Tasmania COVID tracing methods', *The Examiner* (online, 7 November 2020) available at https://www.examiner.com.au/story/7002549/what-are-they-using-the-data-for-concerns-over-covid-tracing/.
[9] Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1429, available at: https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf.
[10] Issues Paper, p 27.
[11] Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1356 available at: https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf.
[12] Ibid at 1392.

public sector employees can make privacy complaints to OVIC about how their employers have handled their personal information.

17. OVIC often sees complaints about interferences with privacy involving employee records. Examples of the conduct my office has received complaints about include:

    a. An organisation that updated an employee's position title to 'WorkCover pension' on its internal and external facing directories. The employee alleged that this resulted in pain and suffering, and damage to their reputation.

    b. A contracted service provider that added a self-service application to all employees' work devices, which did not appropriately secure their personal information, meaning it was visible to other employees. The information included the employee's tax file number; bank details; phone numbers; and the names and ages of their children and spouse. The employee alleged that this resulted in pain and suffering, and concern for their family's safety.

    c. An organisation that inadvertently sent an employee's recruitment information, including their name; address; phone numbers; email address; and certified copies of their drivers' licence; Passport; Medicare card; and tertiary qualifications, to other employees during a period of recontracting. The employee alleged that this resulted in pain and suffering, concern about further dissemination, ostracisation, and inappropriate workplace behaviours.

    d. An organisation that collected an employee's personal and sensitive information from their work computer, including photos; videos; and other information relating to the employee and their family. The organisation then used this information in disciplinary action that led to the employee's termination. The employee alleged that this resulted in pain and suffering, and loss of earnings.[13]

18. At present, these sort of acts and practices would most likely be subject to the employee record exemption, and not prohibited under the Privacy Act. It is our view that most Australians would expect their employer to protect their privacy.

19. OVIC's view is that this exemption should be removed to ensure that employee records are protected by the Privacy Act and also to ensure that employees have appropriate avenues to make privacy complaints where necessary. Removing the exemption would also align the Privacy Act to international jurisdictions such as the European Union, the United Kingdom and New Zealand.

Political parties' exemption

20. The Privacy Act exemption for political parties raises a number of concerns relating to their information handling practices. Political parties collect personal information about voters from a range of sources without their knowledge and consent, including social media and third-party data brokers. Combined with personal information contained in electoral rolls, political parties are able to build large databases with detailed information on voters. As political parties do not have obligations under the Privacy Act, they are not required to inform voters of the ways in which they collect their personal information, nor are they required to specify how that information will be

[13] Kerig v Victoria University (Human Rights) [2020] VCAT 469.

used and disclosed. Therefore, voters often are not aware of how their personal information is managed by political parties.

21. Access to detailed voter profiles enables political parties to engage in targeted political campaigning, which has the potential to negatively impact democracy. Targeted campaigning not only inhibits informed political debate, it also restricts voters' ability to make informed decisions. The misuse of voters' personal information by political parties in past elections has highlighted the need for restrictions on political advertising.[14] There are also concerns around the risk of foreign interference in elections as political parties are not required to have robust data security measures in place to protect the large amounts of personal information that they hold. Additionally, the lack of adequate security protections increases the likelihood of cyber-attacks.[15]

22. Given these risks, political parties should be subject to the Privacy Act. In addition to protecting individuals' information privacy rights, removing the exemption would increase transparency and accountability in political parties' information handling practices and would enhance trust in the democratic process. The Privacy Act would also be more closely aligned with comparable international jurisdictions such as New Zealand, the United Kingdom and Hong Kong.[16]

Notice of collection of personal information

23. Notice of collection is a key tenet underpinning many privacy laws, including the Privacy Act and the PDP Act. As noted in the Issues Paper, the primary function of providing notice is to enable individuals to understand certain details about the collection of their personal information, such as the purpose for which an entity is collecting and will use or disclose their information, and to whom their information may be disclosed, amongst other matters.

24. This is important as it helps to set and manage individuals' expectations about how their personal information could potentially be used, particularly for secondary purposes. As in the PDP Act, one of the many legal bases for the secondary use and disclosure of personal information under the APPs is where the individual would reasonably expect the APP entity to use or disclose their information for that secondary purpose, and that purpose is related to the primary purpose (APP 6.2(a)).[17] Informing individuals of potential secondary uses or disclosures as part of a collection notice helps ensure that those individuals then have a reasonable expectation that their information will be used or disclosed for those secondary purposes, thereby helping to prevent misunderstandings or privacy complaints arising.

25. Notice also plays an essential role in the context of consent. While the concepts of notice and consent are distinct, notice provides individuals with the information they need to make informed and meaningful decisions about whether or not to provide their consent, either for the collection of certain types of personal information (namely, sensitive information), or to certain uses and disclosures of their information. Notwithstanding the challenges of the traditional notice and consent model (which are further discussed below), OVIC considers that notice remains an important tool for individuals' ability to exercise control over their personal information.

---

[14] Marian Sawer, 'After Clive Palmer's $60 million campaign, limits on political advertising are more important than ever', *The Conversation* (online, 21 May 2019) available at: https://theconversation.com/after-clive-palmers-60-million-campaign-limits-on-political-advertising-are-more-important-than-ever-117099.

[15] David Wroe, *'Democracy at stake': Parties warned Australia at risk of US-style cyber manipulation*, *Sydney Morning Herald* (online, 25 April 2019) available at: https://www.smh.com.au/federal-election-2019/democracy-at-stake-parties-warned-australia-at-risk-of-us-style-cyber-manipulation-20190424-p51gu3.html.

[16] Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1319, available at: https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf.

[17] The equivalent exception in the IPPs is IPP 2.1(a).

26. Another purpose of notice (along with privacy policies) is to promote transparency in entities' information handling practices. In relation to the notice requirement in the PDP Act, Bell J noted in *Jurecek v Director, Transport Safety Victoria* [2016] that:

> *The main purpose of the notification requirement in IPP 1.3 is to promote governmental transparency and respect for the autonomy and dignity of individuals with respect to their personal information*.[18]

27. Being transparent and informing individuals about relevant matters relating to their personal information helps entities to build and maintain public trust, and to develop social licence to collect, use and disclose the public's personal information. Further, the requirement to provide notice forces entities to turn their mind to why they are collecting personal information. Entities need to consider the reasons for collecting, using and disclosing personal information, in order to be able to explain to individuals those matters required by APP 5.2.

Strengthening notice requirements

28. Given the importance of notice and the concerns identified in the Issues Paper, OVIC supports, in principle, strengthened notification requirements; in particular, the Australian Competition and Consumer Commission's Digital Platforms Inquiry recommendation in relation to notice being concise, transparent, intelligible, easily accessible and readily understood.[19] This is similar to Article 12 of the GDPR, which states that when providing information to individuals about the handling of personal information, it should be done in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'.[20]

Third party collections

29. As principles-based legislation, both the PDP Act and the Privacy Act require regulated entities to take 'reasonable steps' to provide notification to individuals, whether personal information is collected directly from the individual or indirectly from a third party. In the case of the PDP Act, this requirement is limited only to the extent that providing notice to an individual whose information has been collected indirectly would pose a serious threat to the life or health of any individual.[21]

30. While providing notice to individuals when their personal information is collected is important, the requirement to take 'reasonable steps' appropriately reflects the reality that in some circumstances, doing so may not be practicable or feasible. Placing requirements or limitations on the uses or disclosures of personal information where an entity is unable to provide notice to the individual (whose information has been collected indirectly)[22] could potentially limit or preclude legitimate purposes for using or disclosing that information – for example, in the context of an emergency.

31. A potential approach to strengthening notification in respect of personal information collected indirectly could be a model similar to Article 14 of the GDPR, which requires entities to provide notice to individuals whose information has been collected indirectly, *unless* one of several exceptions applies – for example, the provision of such information is impossible or would involve a disproportionate effort. In this instance, entities are still required to take appropriate measures to protect individuals' right to be informed about the collection and proposed uses and disclosures of

[18] VSC 285 (11 October 2016), [120].
[19] Recommendation 16(b) of the Digital Platforms Inquiry report.
[20] Article 12, Chapter 3 of the GDPR.
[21] IPP 1.5 in the PDP Act.
[22] Issues Paper, p 39, question 23.

their personal information, including by making the information required in a notice publicly available.[23]

Consent to collection, use and disclosure of personal information

32. As with notice, consent is a key principle of many privacy laws. Traditionally, it has been an important mechanism to enable individuals to exercise control over their personal information. However, for consent to be meaningful, five elements need to be satisfied: it must be voluntary, informed, specific, current, and provided by an individual with the capacity to consent.[24] In OVIC's view, the ability for individuals to provide truly meaningful consent is increasingly challenged in today's digital environment, particularly in the context of new and emerging technologies such as AI and IoT. The complexity of different networks, systems, information flows and parties involved in the collection, processing and handling of personal information increasingly renders the binary 'yes' or 'no' consent process at the beginning of a transaction less and less meaningful in today's modern world.

Artificial intelligence and Internet of Things

33. The nature of AI, for example, often makes it difficult – if not impossible – for entities to know how personal information may be used by an AI system in the future. This raises the risk of excessive data collection or vague, broad and bundled collection notices in an attempt to 'catch-all'. This undermines individuals' ability to consent to *specific* uses of their personal information, one of the elements of consent. Bundled consents can also undermine the voluntary nature of consent, as they can coerce individuals to agree to a variety of uses and disclosures in exchange for a service.

34. The complexity of processes surrounding AI can also mean that entities deploying such systems have difficulty in understanding how the AI works, let alone explaining such processes to individuals in such a way that they are able to provide informed consent. Further, even where individuals are informed about how an AI system uses their personal information, many will lack the necessary knowledge to properly understand the implications for their personal information. If individuals do not fully understand how AI applications or algorithms operate, their ability to exercise choices about their personal information and provide informed consent in the context of AI is diminished.[25]

35. Consent is similarly challenged in the context of IoT. For example, where IoT devices are present in shared spaces such as smart cities, smart homes or connected cars, such devices often do not have interfaces or input mechanisms such as screens or keyboards, meaning individuals generally do not have the opportunity to provide consent at all, let alone meaningful consent. Requiring consent for certain uses and disclosures of personal information from an IoT device in order to access a service or physical space would similarly not be meaningful, as the consent would not be truly voluntary.[26]

General comments on consent

36. These issues and challenges are equally relevant in other, broader contexts, not just in relation to technology. Consent, as a concept, places the responsibility on the individual to inform themselves

[23] Article 14, subsection 5(b), Chapter 3 of the GDPR.
[24] For more information about the five elements of consent, see OVIC's *Guidelines to the Information Privacy Principles*, available at: https://ovic.vic.gov.au/book/key-concepts/#Consent.
[25] See OVIC's *Artificial intelligence and privacy* issues paper for more information about how AI challenges consent, available at https://ovic.vic.gov.au/resource/artificial-intelligence-and-privacy/. See also OVIC's *Submission in response to the Artificial Intelligence: Australia's Ethics Framework Discussion Paper*, 31 May 2019, available at: https://ovic.vic.gov.au/resource/submission-to-diis-on-artificial-intelligence-australias-ai-ethics-framework-discussion-paper/.
[26] See OVIC's *Internet of Things and privacy* issues paper for more information about the challenges of consent, available at: https://ovic.vic.gov.au/resource/internet-of-things-and-privacy/.

of the way in which their personal information will be handled, which, as demonstrated above and more generally, can be difficult.

37. Moreover, it is only one of several legal bases that entities can rely on under the APPs to collect, use and disclose personal information. Where another legislative authority exists to allow entities to collect, use and disclose personal information, seeking consent in such instances may appear disingenuous to the individual, if their personal information will be collected, used or disclosed regardless of whether or not consent is provided.

38. Notwithstanding the challenges of ensuring it is meaningful and the existence of alternative legislative authorities, OVIC recognises that consent remains a valuable means for individuals to be able to control who collects their personal information and how it is used and disclosed. As noted in the Issues Paper, this is increasingly important to the Australian public, as reflected in the OAIC's Australian Community Attitudes to Privacy Survey 2020.[27]

39. This sentiment has been raised over the course of OVIC's work with various stakeholders. Members of OVIC's Youth Advisory Group,[28] for example, have raised the importance of consent, particularly that consent should be sought before personal information is collected,[29] regardless of whether or not this is required by privacy legislation.

40. Consent was also a recurring theme in research conducted by Cultural and Indigenous Research Centre Australia on behalf of OVIC in 2020, which explored Aboriginal participants' perspectives on the collection, use and disclosure of their personal information. Aboriginal participants noted the need for consent (and notice) when their information is shared, and were uncomfortable or believed it was unfair when their consent was not sought before a disclosure or secondary use.[30]

41. While consent does and will likely continue to play an important role in information privacy regimes, OVIC is of the view that consent could potentially be supplemented by other mechanisms to enhance privacy protections, particularly where personal information is collected, used and disclosed by private entities that profit significantly from individuals' information.

42. For example, the concept of 'No-Go Zones' – essentially collections, uses or disclosures of personal information that are prohibited in certain circumstances, irrespective of consent – could be worth exploring as a way to protect against certain practices that society considers to be inappropriate and should therefore be precluded. Limiting certain purposes would serve to protect individuals' personal information in a way that does not place the onus on the individual to protect their privacy. Further, constraining purposes for use and disclosure is increasingly becoming more pertinent given the risk of harm to individuals arising from modern data practices – for example, micro-targeted advertising, as discussed above.[31]

43. In suggesting improvements to protection mechanisms, it is also worth referring to 'consent fatigue', the process whereby continually asking for consent for data collection has a corrosive effect on the use of online resources and in fact diminishes the power individuals have over their

---

[27] Issues Paper, p 50.
[28] More information on OVIC's Youth Advisory Group is available at: https://ovic.vic.gov.au/privacy/for-the-public/privacy-for-young-people/youth-advisory-group/.
[29] See OVIC's *Submission: Privacy and Children*, 30 September 2020, available at: https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.
[30] OVIC will release a paper based on this research in early 2021.
[31] For further discussion on No-Go Zones, see OVIC's blog posts on this topic, available at: https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-1/ and https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-2/.

information by overwhelming them with notices requiring their attention.[32] Growth in consent fatigue is one reason alternative protection mechanisms for privacy merit consideration.

Control and security of personal information

44. OVIC considers that the security requirement under the Privacy Act – that APP entities take reasonable steps to protect the personal information they hold from misuse, interference, loss, unauthorised access, modification or disclosure – is appropriate to protect personal information of individuals. This is similar to an equivalent requirement in IPP 4 of the PDP Act.[33]

45. The requirement to take reasonable steps (rather than implement prescriptive security controls) supports a risk-based approach towards the security of personal information, as it requires organisations to implement measures proportionate to the potential privacy risks to individuals and the potential harm caused to them.

46. This approach recognises the diverse nature of different entities, their unique operating environments, information holdings, and the types of privacy risks that may arise. The principle of 'reasonableness' underpinning APP 11 also allows entities to scale measures up and down as required, which is important given the dynamic nature of the digital environment and the technologies that entities may adopt.

47. As entities' information holdings and the value of data grows, ensuring entities adhere to the security requirement in APP 11 will be increasingly pertinent, particularly in light of growing harmful risks arising within the digital world, such as cyber-attacks and data breaches. The OAIC will need to play an increasingly important role in ensuring Australia is able to take advantage of the information economy, through the protection of personal information and promotion of public trust in entities' handling of such information. As noted previously in this submission, it is imperative that the OAIC be appropriately resourced to do this.

Notifiable Data Breaches scheme

48. OVIC recognises the value that the Notifiable Data Breaches (**NDB**) scheme has had in raising awareness of the importance of data security amongst regulated entities, as well as other bodies not subject to the scheme. The increase in data breach notifications to OVIC (which were voluntary prior to the introduction of the Information Security Incident Notification Scheme in October 2019) has coincided with the implementation of the NDB scheme.[34]

49. OVIC considers the NDB scheme has also promoted greater transparency and accountability within entities in relation to data breaches. Importantly, the scheme has also helped minimise the potential harm to individuals affected by a data breach. By notifying affected individuals (where appropriate in the circumstances), those individuals are able to take necessary steps to protect their personal information.

50. Overall, OVIC considers that the NDB scheme has been effectively administered and commends the OAIC for the significant work and effort undertaken in doing so.

---

[32] Bart Schermer, Bart Custers and Simone Van der Hof, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' (2014) 16 *Ethics Inf Technol* 171, 171–182 available at https://doi.org/10.1007/s10676-014-9343-8.
[33] IPP 4.1 requires an organisation to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure'.
[34] The Information Security Incident Notification Scheme applies to regulated entities subject to Parts 4 and 5 of the PDP Act and requires those entities to notify OVIC of incidents that compromise the confidentiality, integrity or availability of 'public sector information' with a 'limited' business impact or higher on government operations, organisations or individuals. For more information see OVIC's website at https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/.

Enforcement powers under the Privacy Act and the role of the OAIC

51. The Privacy Act provides a range of enforcement powers to the OAIC. While these could be strengthened through the addition of new enforcement powers, effective enforcement of the Privacy Act is also impacted by the amount of resourcing provided to the OAIC to enable it to carry out its statutory functions.

52. OVIC suggests that the review team consider OAIC's and its predecessors' expanding privacy responsibilities over the last four decades, as described in their annual reports.[35] These reports show that the role of Australia's federal privacy regulator has grown immensely over this time. For example, in the first year of the Privacy Act's operation, the privacy functions of the Human Rights and Equal Opportunity Commission extended to providing advice, conducting audits, and handling 59 complaints about federal government agencies.[36] It estimated that it spent $1.6 million carrying out these activities[37] – the equivalent of $3.4 million today.[38]

53. In contrast, in 2019-20, the OAIC's privacy functions included providing advice, conducting audits, managing a data breach notification scheme, exercising a wide range of regulatory powers, conducting court proceedings against Facebook, and handling 2,673 privacy complaints. As well as regulating the public sector, it also has the larger task of regulating Australia's private sector, and large global businesses that collect personal information in Australia. Its total expenses were reported to be $23 million – but this amount also includes its work in its role as Australia's freedom of information regulator.

54. In light of its growing responsibilities, it is crucial that the OAIC is appropriately resourced to effectively carry out its regulatory functions, including its complaint handling and determination functions.

Interaction between the Privacy Act and other regulatory schemes

55. OVIC acknowledges that, as noted in the Issues Paper, the existence of multiple frameworks regulating different elements of privacy and types of information has the potential to cause confusion for the community and industry.[39]

56. While greater consistency of protections under different privacy regimes would have its benefits, OVIC is of the view that given the nature of entities covered by the Privacy Act – in particular private sector entities – there is a strong argument for the Privacy Act to have separate privacy protections to address the risk posed by such entities, whose data holdings can have the biggest impact on individuals' lives.

57. For many private sector entities, a significant profit-making activity is the collection, use and disclosure of individuals' personal information. Thus, there is a greater risk of these entities over-collecting and misusing personal information. These privacy risks are likely to increase as the information economy grows and the value of personal information increases. As such, holding the private sector to a higher standard of privacy protection would be valuable for the public, and would ensure that the public's information privacy rights are upheld. In turn, this would help build public trust in the private sector's information handling practices.

---

[35] Human Rights and Equal Opportunity Commission, *Annual Report 1989-90* (Report, 1989-90*)*; Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report 1999-2000 (*Report, 1999-2000*)*; Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report 2009-2010* (Report, 2009-2010*)*; Office of the Australian Information Commissioner, *Annual Report 2019-20* (Report, 2019-20).

[36] Human Rights and Equal Opportunity Commission, *Annual Report 1989-90*, (Report, 1989-90) 90.

[37] Ibid at 125.

[38] See https://www.rba.gov.au/calculator/annualDecimal.html.

[39] Issues Paper, p 83.

Thank you once again for the opportunity to provide comment on the Issues Paper. My office will watch the progress of the review with interest, and looks forward to any further opportunities to provide input into the review.

I have no objection to this submission being published by the Attorney-General's Department without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but would be happy to adjust the timing of this to allow the Department to collate and publish submissions proactively.

If you have any questions about this submission, please do not hesitate to contact me directly or my colleague Anita Mugo, Senior Policy Officer, at Anita.Mugo@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner