Electronic Frontiers
AUSTRALIA

w www.efa.org.au
e email@efa.org.au
@efa_oz

26 November 2020

Attorney-General Department
4 National Circuit
BARTON ACT 2600

By Email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: REVIEW OF THE *PRIVACY ACT 1988*

We appreciate this opportunity to make submissions in relation to the review of the *Privacy Act 1988* ("**the Act**").

Electronic Frontiers Australia's ("**EFA**") submission is contained in the following pages.

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Angus Murray
Chair of the Policy Committee,
Electronic Frontiers Australia

Introduction

This submission responds to each of the sixty-eight (68) questions posed within the Issues Paper; however, this submission must be read in the context of EFA's long-standing and overarching submission that Australians ought to be afforded a base-line protection of their human rights by the introduction of a federal and enforceable human rights framework as well as a tort for serious invasion of privacy.

In this context, and as the Issues Paper identifies, Australians care about their personal information "with almost 9 in 10 respondents indicating they want more choice and control over their personal information"[1]. It ought to be clear, from observation of both domestic and international examples, that privacy and the broader landscape of human rights protections is necessary and desirable to protect the Australian community. As has been expressed by Angus Murray, Chair of EFA's Policy Committee, on numerous occasions across a variety of fora, the right to privacy is a core human right and it is underpinned by the premise that founds all human rights; humans ought to be able to operate with autonomy and dignity.

We respectfully appreciate the review of the Act; however, it is our core proposition that issues with the Act ought to be addressed in the broader landscape of modernising Australians' human rights protections and aligning those protections with all other liberal democracies and international law, including the *International Covenant on Civil and Political Rights* and the *International Covenant on Economic, Social and Cultural Rights.*

Objectives of the Privacy Act

1. *Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?*

In our view, the objects of the Act as outlined in s. 2A of the Act ought to be expanded and we agree with the DI Report. The expansion needs to properly encapsulate both the use of personal, sensitive and/or health information in business in a direct sense and the aggregation and analysis of that data. We respectfully submit that the context of personal information has significantly changed with the rapid onset of data analytics and the computational processes that are capable of being deployed against consumers. The increasing use of advanced computational processes, including artificially intelligent advertising, marketing and monitoring applications, requires a heightened focus on the importance of the protection of privacy and the greatly heightened risks to privacy posed by these technological advances

We also respectfully consider that the Act does not sufficiently import Australia's international obligations in relation to privacy and the Act needs to be expanded to protect individuals (by an

[1] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (September 2020) 7.

enforceable civil and/or criminal remedy) from unlawful interference by government, business and other individuals.

Definition of personal information

2. *What approaches should be considered to ensure the Act protects an appropriate range of technical information?*

3. *Should the definition of personal information be updated to expressly include inferred personal information?*

4. *Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?*

5. *Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?*

We submit that the definition of 'personal information' is outdated and requires amendment. We submit that 'personal information' ought to include:

- inferred data (including but not limited to technical data and metadata);
- information that directly or indirectly identifies an individual or can be used, in aggregation with other data, to identify an individual; and
- information that can be used in combination with any other data (including in any automatic processing) that may identify an individual.

We are concerned that the decision in *Privacy Commissioner v Telstra Corporation Limited*[2] has created an inappropriately narrow construction of the definition of personal information. Although the Court in that matter determined that the information in question was "about a service" rather than "about an individual" that information, using basic aggregation, could reasonably identify an individual. It is necessary to ensure that the definition of 'personal information' is robust in the face of advancing technology and that the definition remains fit for purpose to the objects of the Act.

Furthermore, we submit that the concept of "about an individual" requires amendment. It is increasingly common for individuals to be identified against a crowd, a big data set or from seemingly unconnectable information. That process of individualisation does not squarely fall within the concept of "about an individual" because the process is in reverse: the data (digital/physical movements, profiles, user history, etc) can be used to identify an individual despite that data not being "about an individual". We respectfully suggest that the definition of 'personal information' should be aligned with the definition of that term as it is contained at Art. 4(1) of the European *General Data Protection Regulation* ("**GDPR**").

[2] [2017] FCAFC 4.

Flexibility of the APPs in regulating and protecting privacy

6. Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

We respectfully submit that the Act ought to be broadened and the APPs ought to apply to all businesses operating, directly or indirectly, in Australia. While we appreciate that the APPs have served a purpose, that purpose must be broadened to ensure that the personal information of all Australians is protected. The context of small business (entities under a turnover of $3m that are not bound to the APPs) has dramatically shifted as a consequence of the advancements in technology and the ubiquitous use of same.

The protection of an Australian's privacy should not depend on the size of the entity they are dealing with. We expect that products sold to us in Australia are safe regardless of their origin. We do not expect to be poisoned by coffee served at a local cafe or by a large multinational chain. The focus of privacy protections should be on those who are being protected.

We respectfully submit that the Act ought to bind all *entities, acts and practices* that, directly or indirectly, collect, use, access or disclose Australians' personal information.

Exemptions

Small business exemption

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

8. Is the current threshold appropriately pitched or should the definition of small business be amended?

a. 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?

9. Are there businesses or acts and practices that should or should not be covered by the small business exemption?

10. Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?

a. *If so, what obligations should be placed on small businesses?*

b. *What would be the financial implications for small business?*

11. Would there be benefits to small business if they were required to comply with some or all of the APPs?

12. Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?

We repeat our response to Question six (6) above. The Act ought to bind all *entities, acts and practices* that, directly or indirectly, collect, use, access or disclose Australians' personal information.

A small business is no more able to sell dangerous products than a large one. Dangerous data practices place Australians' privacy in jeopardy and should be equally prohibited no matter the size of the entity we are dealing with.

In specific response to Question twelve (12), it is our view that "consent" is a vexed issue (and discussed later in this submission). It is important that Australians', who often are ill-informed or otherwise unaware of the content of the consent being provided, are protected in any event by a base-line of privacy law. This must particularly be the case where business, at any scale, trades in personal information. In this context, we agree with the Privacy Commissioner's recommendation for "*the removal of these consent provisions on the basis the provisions were 'clumsy and complicated*'".

Employee records exemption

13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?

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

15. Should some but not all of the APPs apply to employee records, or certain types of employee records?

We note the reference to *Lee v Superior Wood Pty Ltd*[3] in the issues paper and, in response to the employee records exemption, it is our submission that such exemptions ought only apply where:

- the person is a current employee;

[3] FWCFB 2946; 286 IR 368.

- compliance is current with the State and Territory privacy legislation, and the *Fair Work Act 2009*; and
- there is free, full and informed consent to the maintenance of the record.

Political parties exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

We submit that the political exemption ought to be abolished. In our opinion, the recent issues with political parties, consultancies and with the spread of misinformation warrant a high degree of caution on the ability for political parties to be exempt from the operation of the Act. The operation of the exclusion of 'registered political party' at s. 6C of the Act and the exemption of political acts or practices done in connection with an election, a referendum or another aspect of the political process by political representatives (MPs and local government councilors), contractors and subcontractors for political parties and representatives, as well as volunteers for registered political parties at s. 7C of the Act ought to be repealed.

In the above context, we do accept that there is a "strong public interest in promoting Australia's system of representative democracy" and we agree with the Australian Law Reform Commission Report 108 that a removal of the exemption for political parties ought also bring the introduction of "*providing limited exceptions for political acts and practices or requiring registered political parties and other entities engaging in political acts and practices to develop information-handling guidelines, in consultation with the then Office of the Privacy Commissioner*"[4].

Journalism exemption

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?

18. Should the scope of organisations covered by the journalism exemption be altered?

19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

We submit that the journalism exemption ought to be abolished. However, we are not opposed a limited exemption being introduced where journalists (in a broad and non-exhaustive definition of that term) are permitted to collect, use and disclose (as those concepts exist in APPs 3, 5 and 6) information necessary for public interest journalism and where that collection, use and disclosure is the subject of a mandatory Code approved and regulated by the Privacy Commissioner.

[4] ALRC, *For Your Information: Australian Privacy Law and Practice* (n 109) 1426.

Notice of Collection of Personal Information

Improving awareness of relevant matters

20. Does notice help people to understand and manage their personal information?

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?

Third party collections

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

Limiting information burden

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

EFA submits that a consistent framework of fundamental privacy protections would both ease regulatory compliance burden and simultaneously limit the information burden on individuals.

Fundamental privacy protections that can be assumed to generally apply would free individuals from investigating for themselves whether or not their privacy is being protected in these fundamental ways, in much the same way that individuals do not need to verify for themselves that their coffee is not poisoned and that bread does not contain asbestos. Indeed, it is considered ridiculous that such a thing would occur, such is the strength of product safety regulations.

Similarly, organisations would be freed from having to verify for themselves every link in their information supply chain contains appropriate privacy protections. In today's world, information management products are generally provided by external suppliers rather than developed in-house, and so the compliance burden for organisations is increased when they are responsible for verifying and disclosing to their customers every aspect of information handling practice that needs to be disclosed. Standard contract terms could simply refer to statutory legislation, much as they do for e.g. collection of GST.

EFA submits that fundamental statutory protections could be assumed to apply and thus would not need to be specially communicated. Individuals would therefore only need to look for disclosure of exceptional circumstances, and organisations would also then only need to expend effort to disclose those exceptional circumstances, reducing their regulatory compliance burden.

Consent to collection and use and disclosure of personal information

Consent to collection, use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

28. Should individuals 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?

29. Are the existing protections effective to stop the unnecessary collection of personal information?

a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?

30. What requirements should be considered to manage 'consent fatigue' of individuals?

We agree that consent is an effective way for people to manage their personal information. Inherently underpinning the concept of privacy are the principles of human autonomy and dignity. We respectfully accept that, even the most informed people (which we return to in the circumstance below described as "the second limb"), may not be troubled by the collection, use and disclosure of their personal information in certain circumstances. However, we consider that the definition of consent ought to be narrowed and a useful example of a narrow definition of consent is contained at Art. 4(11) of the GDPR which provides that:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

In this context, we consider that consent *must* be, in all of the relevant circumstances, fully and freely given by an individual who is informed and where the consent is specific and express. The difficulty that often presents itself with a consent approach in this context is twofold:

- firstly, it is difficult to ensure that the individual is fully informed; and
- secondly, there is often no choice other than to provide consent.

In the first limb, there is a need to enhance the Act to empower and fund the Privacy Commissioner to educate Australians as to the importance of their personal information and the bargain of trust that is being brokered with the entity that is acquiring said consent. This is often lost to the rhetoric that providing personal information is exchanged with convenience and/or that the consent being provided can do no tangible or direct harm. The prevalence, which is only likely to increase, of identity theft and the unquantifiable and significant harm that may be suffered by misuse of personal information must be properly understood before Australians can fairly bargain with their personal information (although we disagree that consent ought to be founded as a contractual right in the context of personal information).

Additionally, most Australians do not have the time to comprehensively read consent notices nor, in many cases, would Australians be able to fully and completely understand the content of those notices. Education must also be supported by requirements for plain language and simplified notices.

In this regard, it is very difficult to be able to fully inform an individual as to the consequence(s) of consenting to the collection, use and disclosure of personal information as the future is inherently unknown. The potential consequence today is not necessarily the same as a consequence that may arise in the future. Information collected about an individual is long-lived, and advances in technology create new risks that were not possible to foresee when the information was collected, rendering informed consent impossible.

In the second limb, the bargain can *never* be fair where there is no option other than to provide consent to access a service. For example, consider an App that requires a user to click 'accept' to the terms and conditions of use, including a consent to the collection, use and disclosure of their personal information. Even in the circumstance where a person is fully informed as to the consequence of providing their consent, there more often than not no option to alter or adjust the consent being given.

Australians should also be able to rely on a fundamental level of privacy protection that does not require constant, active vigilance on their part. We are able to buy bread without worrying if every loaf may be poisoned. We do not need to haggle with every vendor for the right to a refund or replacement if the goods are faulty. It is entirely appropriate for the government to establish certain fundamental privacy protections that we are not required to read and consent to with every transaction, and that we cannot be swindled out of by an unscrupulous party. This is common practice in other areas of the law and we submit that this principle should be adopted to establish certain fundamental privacy protections.

Exceptions to the requirement to obtain consent

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?

We do not offer comment in relation to the fitness of the current general permitted situations and general health situations.

Pro-consumer defaults

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

We completely agree that entities collecting, using and disclosing personal information should be required to implement pro-privacy defaults.

Obtaining consent from children

33. Should specific requirements be introduced in relation to how entities seek consent from children?

We repeat our response under the heading "Consent to collection, use and disclosure of personal information" and submit that these protections ought to be amplified in the context of children.

The role of consent for IoT devices and emerging technologies

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

We respectfully draw attention to the Australian Communications Consumer Action Network Internet of Things Position Statement released in October 2020 and the recommendations contained therein.[5]

Inferred sensitive information

35. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

We repeat our response under the heading "Consent to collection, use and disclosure of personal information".

[5] See also: Roger Clarke, *Is Your Television Spying on You? The Internet of Things Needs More Than Self-Regulation* (accessed 18 November 2020) available at URL: http://www.rogerclarke.com/II/IoTCJ.html.

Direct marketing

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

We repeat our response under the heading "Consent to collection, use and disclosure of personal information"

Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

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

40. Should there be some acts or practices that are prohibited regardless of consent?

We repeat our response under the heading "Consent to collection, use and disclosure of personal information".

Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

We agree with the scope and effect of Part VIA of the Act and do not propose any amendment to the same.

Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

We repeat our response under the headings "Definition of Personal Information" and "Consent to collection, use and disclosure of personal information".

Control and security of personal information

Security and retention

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

We consider that the "right to erasure" as expressed at Art. 17 of the GDPR ought to be introduced to Australian law. Personal information ought not be retained for any period longer than is reasonably necessary to achieve the purpose of the collection and security favours a default that data is not retained longer than reasonably necessary. We respectfully submit that a baseline proposition that personal information ought to be deleted on the earlier of the completion or cessation of the reason for which it was collected or twelve months (12) unless the data subject has provided full, free and informed consent that the data be stored for a longer duration that does not exceed seven (7) years.

Access, quality and correction

45. Should amendments be made to the Act to enhance:

a. transparency to individuals about what personal information is being collected and used by entities?

b. the ability for personal information to be kept up to date or corrected?

Yes, it is fundamentally important to the integrity of a privacy regime to ensure that the collection, use and disclosure of personal information is clearly and expressly transparent.

Right to erasure

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

We consider that the "right to erasure" as expressed at Art. 17 of the GDPR ought to be introduced to Australian law. Personal information ought not be retained for any period longer than is reasonably necessary to achieve the purpose of the collection and security favours a default that data is not retained longer than reasonably necessary. We respectfully submit that a baseline proposition that personal information ought to be deleted on the earlier of the completion or cessation of the reason for which it was collected or twelve months (12) unless the data subject has provided full, free and informed consent that the data be stored for a longer duration that does not exceed seven (7) years.

Overseas data flows and third party certification

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

a. Are APP 8 and section 16C still appropriately framed?

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

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

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

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

We acknowledge that, as a consequence of the interconnected nature of the digital world, data is shared overseas. We agree that equivalent protection ought to be required for overseas sharing. We are concerned to ensure that data does not become commodified and exchanged internationally as this commodification places monetary value on human rights which is unacceptable. This also causes potential reform issues as regards to transfer pricing and revenue consequences associated with overseas data flows.

In our view, noting the issues expressed in this submission, that overseas data flows could be address by transparency, privacy by design and free, full and informed consent to the overseas sharing of data.

Enforcement powers under the Privacy Act and role of the OAIC

53. *Is the current enforcement framework for interferences with privacy working effectively?*

54. *Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?*

55. *Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?*

    a. *If so, what should these enforcement mechanisms look like?*

EFA submits that the greatest impediment to effective use of existing enforcement powers under the Privacy Act stem from the chronic underfunding of the OAIC.

A properly funded OAIC would likely do much to forestall the need for a direct right of action, though a direct right of action should also be available for those few times when the OAIC is not the appropriate party to deal with the specific circumstances of a case. EFA submits that, ideally, the vast majority of cases would be adequately dealt with by the OAIC and a rare and infrequent use of a direct right of action would indicate that the enforcement powers were being used appropriately.

Direct right of action

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

EFA submits that a direct right of action should be framed as an alternate option to action by the OAIC (or other regulatory bodies) that acts as a check on the success or failure of regulators. Recent Royal Commissions[6] have highlighted that, on occasion, regulators have been unable to adequately protect individuals and that an alternate pathway is sometimes required to ensure justice.

EFA submits that successful action by the government in protecting privacy would alleviate the need to make use of a direct right of action. A direct right of action would thus act as a useful indicator of how well privacy protections are working and would highlight areas that may need further adjustment.

Statutory tort

57. Is a statutory tort for invasion of privacy needed?

58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

59. What types of invasions of privacy should be covered by a statutory tort?

60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

EFA has long been a supporter of a statutory tort for serious invasion of privacy as recommended by the Australian Law Reform Commission.[7]

---

[6] See, e.g. 'Financial Services Royal Commission - Home' <https://financialservices.royalcommission.gov.au/Pages/default.html>; 'Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability', *Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability* <https://disability.royalcommission.gov.au/royal-commission-violence-abuse-neglect-and-exploitation-people-disability>; 'Royal Commission into Aged Care Quality and Safety', *Royal Commission into Aged Care Quality and Safety* <https://agedcare.royalcommission.gov.au/royal-commission-aged-care-quality-and-safety>.

[7] 'A Statutory Cause of Action for Serious Invasion of Privacy', *ALRC* <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/4-a-new-tort-in-a-new-commonwealth-act/summary-138/>.

EFA submits that this is a well canvassed area of privacy law and that the recommendations of the ALRC have been broadly supported for many years. There is no need to re-investigate this issue in detail once again, and to do so could be interpreted as an attempt to obstruct and delay action on this issue.

Notifiable Data Breaches scheme – impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?

64. Has the NDB Scheme raised awareness about the importance of effective data security?

65. 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?

EFA is broadly supportive of the NDB Scheme and believes that it has helped to inform the public of the prevalence of data breaches and the risk to privacy that data collection provides.

EFA believes that the NDB Scheme should be further enhanced to ensure that all people whose data is subject to a breach are informed in a timely manner so that they can take appropriate steps to protect themselves from further harm. Individual risk profiles are different and the organisation subject to a data breach is frequently unaware of these individual risk profiles.

It is unreasonable to expect individuals to provide this, often sensitive, information to organisations. Organisations are therefore frequently unable to accurately predict if a data breach is likely to cause an individual serious harm. Ironically, this places organisations at risk of non-compliance with the NDB Scheme.

Individuals are best placed to make an assessment of whether a data breach is likely to cause them serious harm and should be provided with the necessary information to be able to make this assessment by an organisation if an organisation is subject to a data breach.

Interaction between the Act and other regulatory schemes

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

67. Is there a need for greater harmonisation of privacy protections under Commonwealth law?

a. *If so, is this need specific to certain types of personal information?*

68. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

EFA submits that the operation of the proposed *Data Availability and Transparency Bill*[8] would potentially bypass and render moot any adjustments made to the *Privacy Act*. Any changes to privacy legislation should not be done in isolation and should take into consideration the operation of other legislation and regulatory schemes.

EFA submits that some privacy risks and concerns are domain specific and that it is appropriate that certain classes of information require special protections. This principle is already recognised by the protections provided for Tax File Numbers, health information, and information provided to the Census, for example.

EFA further submits that adding special protections for particularly sensitive information is not incompatible with a framework that provides certain fundamental privacy protections that apply to all personal information by default. EFA submits that a layered framework of increased protections for information based on increased sensitivity is a well-recognised approach already used in other contexts, such as sensitive and security classified information. EFA submits that a similar approach could be used to provide a unified framework for information privacy protections that would also aid understanding of compliance obligations.

We trust that this submission is of assistance.

[8] See, e.g. https://www.datacommissioner.gov.au/data-sharing/legislation