27 November 2020

Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600
PrivacyActReview@ag.gov.au

To the Attorney-General's Department,

Submission into the Privacy Act Review – Issues Paper

We would like to thank you for the opportunity to provide feedback on the Privacy Act Review – Issues Paper and commend the government for continuing to engage and consult with community and other stakeholders to ensure privacy settings empower consumers and protect their privacy.

About HALC:

The HIV/AIDS Legal Centre (HALC) is the only not-for-profit, specialist community legal centre in Australia. We provide free and comprehensive legal assistance to people in NSW with HIV or Hepatitis-related legal matters and undertake Community Legal Education and Law Reform activity in areas relating to HIV and Hepatitis.

Submissions

Q1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

HALC agrees with the ACCC's recommendations to amend the objects of the Privacy Act to put greater emphasis on 'empowering consumers to make informed choices.'[1] We recommend the replacement of section 2A(b) with the following object:

'to promote the right of individuals to make informed choices about their privacy'

Creating an environment that promotes the right for individuals to choose how their information is collected, used and disclosed facilitates trust between individuals and entities. This facilitation and strengthening of trust will allow individuals to feel more comfortable sharing their personal information, when they wish to do so, and in return will

[1] Digital Platforms Inquiry – Final Report, ACCC https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, page 35.

allow entities to carry out their functions and activities with greater transparency, accountability and efficiency.

The current privacy framework does not create a trusting environment as is highlighted in the 2019 Deloitte Privacy Index which found that 46% of consumers are likely to provide false information if they can with 81% of people sighting privacy as their reason for providing false information.[2] This may have significant implications on entities functions and activities if nearly 50% of their data is not accurate.

Q3. Should the definition of personal information be updated to expressly include inferred personal information?

The definition of personal information should expressly include inferred personal information, or at the very least inferred sensitive information. As the analysing of big data becomes easier for large entities and more intrusive for individuals, it is essential for the Act to recognise an individual's right to consent to the collection and use of this information. This has been recognised by the United Nations High Commissioner for Human Rights who have recognised that the right to privacy is broad and is extended to metadata that is analysed and aggregated to reveal insights into "an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication."[3] The report concludes that the collection and use of such data without the consent of the individual would constitute an interference with privacy.

It is widely accepted that entities have access to a large range of metadata in which they may infer sensitive information from, such as a person's health status, sexual orientation or racial/ethnic origin. This information could be inferred by entities through marketing cookies, geo-locations and general demographics. For example, a person's sexual orientation may be inferred by Facebook likes and general interactions on social media sites[4]. Similarly, a person's health condition such as a person's HIV status may be inferred by the medication they are searching for or purchasing, the geo-locations of the health services they are accessing and the geo-location of mental health services. There is also a threat that the inferred information collected by the entity is not accurate or may be misleading and if not currently included within the definition of personal information may not give rights to individuals to amend this information.

Under the current provisions of the Act, sensitive information may only be collected with the consent of the individual unless there are exceptional circumstances which arguably would rarely apply to inferred sensitive information if the definition were to be expanded.

[2] 'Trust: Is there an app for that?', Deloitte Australian Privacy Index 2019 https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf, page 16.
[3] 'The right to privacy in the digital age', Report of the Office of the United Nations High Commissioner for Human Rights, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf page 6.
[4] 'Private traits and attributes are predictable from digital records of human behavior' Proceedings of the National Academy of Sciences of the United States of America, https://www.pnas.org/content/pnas/110/15/5802.full.pdf .

Similarly, the use and disclosure of sensitive information may only occur with the consent of the individual unless there are exceptional circumstances.

We believe that the same privacy principles should be applied to any inferred personal and sensitive information giving individuals the right to consent to its collection and to access and amend the information when collected lawfully. The collection of inferred sensitive information is discussed further later in these submissions.

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

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

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

HALC strongly believes that the collection, storage, use and disclosure of health and biometric information for all employment purposes should be regulated under the Privacy Act. Although some protections exist, such as federal anti-discrimination laws which regulate the unlawful use of personal information for purposes of discrimination, we believe greater protections for the collection, use, storage and disclosure of health and biometric information by employers is necessary.

Pre-employment health checks are a common occurrence in a range of employment areas and employees may feel obliged to disclose health information to their employer despite a lack of protections surrounding the storage and use of the information. For example, HALC are often asked to advise on the disclosure of a person's HIV status to employers as questions about medication and health conditions commonly appear in pre-employment health checks. Unnecessary disclosure of a person's HIV status may lead to a private sector employer sharing this information with a potential employer of a past or current employee under the current exemption. As a highly stigmatised condition the disclosure of a person's HIV status may lead to discrimination of the employee without their knowledge and therefore a lack of any remedy available.

The application of the employee records exemption within the act for the private sector is also inconsistent with public sector employees where protections exist. We believe these protections should be expanded due to the lack of any justification as to this exemption for private sector entities and due to the highly sensitive nature of the information provided.

HALC strongly recommends the inclusion of a provision within the act that acknowledges the responsibilities of employers who collect health information for pre-employment purposes. The provision should acknowledge that any health information collected for pre-

employment purposes by a future or current employer may only be collected if relevant to determining if the individual can complete the inherent requirements of the job.

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

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

Question 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?

Most notices from entities outlining how personal information will be collected, used and disclosed do not currently meet client expectations. The findings of the Office of the Australian Information Commissioner (OAIC) indicate that only 20% of Australians read privacy policies and understand their contents.[5] We also wish to highlight the findings of the OAIC's report that identifies that consumers want privacy policies that are easier to understand, feature standard and simple language and use icons as visual prompts.

We assert that entities that have the time and resources to collect non-essential personal information for their entity should also be in a place to effectively manage consent and ensure effective practices and policies to do so are in place. These requirements may include, but are not limited to, an initial opt-in notice to consumers for the collection of any non-essential uses of their information, non-English speaking translations of the privacy policy and compliance with best practice guidelines on making these resources accessible to people with disabilities.

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

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

Question 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?

[5] 'Australian Community Attitudes to Privacy survey 2020' Office of the Australian Information Commissioner https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf, page 5.

Meaningful consent is an essential component in creating trust between consumers and entities. As the public continue to learn more about how personal information is collected and used by entities, consent and trust should play an increasing role in ensuring transparency and accountability. Research continues to demonstrate that consumers understanding of consent is vastly different to the actions of entities.

The practice of bundled consent by entities is of concern as individuals may be required to consent to a range of collection, uses and disclosures of their personal information and be refused services if they do not agree with a single clause in which non-essential personal information is to be collected. Whether or not this practice gives individuals the opportunity to provide real and free consent are drawn into question.

Expectations of clients are not being met regarding what is being consented to within bundled privacy policies and/or terms and conditions notices. The Deloitte privacy index 2020 found that only 37% of consumers agreed 'that they have provided an organisation with valid consent for non-essential processing when that processing was mentioned by the terms and conditions and/or privacy policy.'[6] In order to address this, we recommend that consumers should be provided with the choice to opt-in to non-essential uses of their personal information as opposed to an opt-out option.

We recommend the Act adopts similar provisions to the European Union's General Data Protection Regulation (GDPR). Article 7 of the GDPR states '*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.*'[7] Requirements that consent be unbundled, intelligible and in plain language should be incorporated within the Act to give individuals the ability to consent only when they understand and have a choice as to what they are consenting to. We continue to assert that entities that have the time and resources to collect non-essential personal information for their entity should also be in a place to effectively manage consent and create safeguard requirements to do so.

Question 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?

[6] 'Opting-in to meaningful consent' Deloitte Australian Privacy Index 2020 https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-australian-privacy-index-2020.pdf page 13.
[7] General Data Protection Regulation, https://gdpr-info.eu/art-7-gdpr/, article 7.

Where consent is refused by an individual to the collection, use or disclosure of non-necessary personal information, an entity should not be given the right to deny them access to a product or service. This measure would create a clear power imbalance between entities and individuals seeking their product or service. We are concerned such measures would disproportionately impact vulnerable groups who may already have a mistrust of entities handling their personal information. Vulnerable groups, such as people living with HIV, are particularly sensitive about the information they provide to entities due to their experience of stigma and discrimination where disclosure of non-necessary information has led to negative outcomes.

Furthermore, The OAIC report found that 59% of Australians have experienced problems with the handling of their personal information in the past 12 months.[8] Australians who have already had negative privacy experiences by entities may be less likely to allow entities to collect, use or disclose non-necessary personal information. We assert that it should be the responsibility of entities to create privacy safeguards to promote individuals to share non-necessary personal information where they see fit, empowering individuals to choose how their personal information is to be handled.

Question 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?

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

The collection of inferred sensitive information is an extremely intrusive practice and may potentially be harmful to individuals where this information is not accurate of misleading.

As indicated above in question 3, we believe that inferred sensitive information should be included within the definition of sensitive information. Similarly, the definition of 'collection' should be updated to reflect the collection of inferred sensitive information. Individuals should have the right to consent to the collection of their inferred sensitive information, especially as individuals would be unaware of what measures are being used to obtain this information.

Where the collection of inferred sensitive information is to be consented to, the notice should clearly describe the type of sensitive information that may be inferred (e.g. health information, ethnicity, political views), what methods are being used to infer such information (e.g. web scraping, geo-locations), and an option for this information to be disclosed to the individual. The collection, use and disclosure of this information should also be an opt-in option only.

[8] Above, n5, page 6.

Question 38. Should entities be required to expressly provide individuals with the option of withdrawing consent?

HALC strongly supports the recommendations of the Consumer Policy Research Centre that individuals should have the option of withdrawing consent to entities that may have access and use of their data.[9] We note that the OAIC guidelines recognise this right, however we believe these provisions should be provided within the Act. We recommend a similar provision found within the GDPR on withdrawal of consent be implemented within the Privacy Act.

The ability and recognition that individuals may withdraw consent will incentivise entities to engage in privacy practices that will offer individuals greater security of their personal information and best practice of the handling of their information.

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

HALC also supports the ACCC's recommendations that the Privacy Act acknowledge the right of individuals to have their personal information erased by entities on request.[10] This provision would recognise the right of individuals to not only withdraw their consent but would ensure entities could no longer use the data to gain any financial benefit.

Erasure of data would give individuals greater control and choice over where and how their data is stored and would provide further incentives for entities to create and enforce strict privacy policies and frameworks. A similar provision exists in the GDPR, brining Australia's privacy law in line with other jurisdictions, allowing entities that expand to European jurisdictions to easily comply with these requirements.

If additional information or citations in relation to this submission are required, please feel free to contact Rhys Evans on rhys@halc.org.au.

Yours sincerely,

Alexandra Stratigos
Principal Solicitor
HIV/AIDS Legal Centre

[9] Above, n1, page 471.
[10] Ibid, page 470.