Australian Computer Society Inc. (ACT)
ARBN 160 325 931

National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Australian Government Attorney General's Department,

ACS response to the October 2021 Review of the Privacy Act 1988 (Cth) Issues paper

10 January 2022

General feedback on Part 2

ACS appreciates the efforts of the Attorney's General's Department to reach out and consult with various community stakeholders on the Privacy Act. It's incredibly complex work, and needs broad and extensive consultation to fully understand the practical compliance risks as well as the ethical and moral considerations required to keep the Act consistent with a free and open society.

With that in mind, a number of our expert members offered commentary on the matters included in the discussion paper. These included the following points, primarily related to Part 2 of the paper:

1. We concur that technical information that can identify an individual should be included within the definition of "about an individual". Electronic fingerprinting techniques are becoming more sophisticated and effective with very sparse information. This, coupled with individuals using or being monitored by electronic devices that are always connected to the Internet, means that technical information is possibly more invasive than personal information consciously input by the individual. We concur with the CSIRO's assessment of the privacy risk and hence the inclusion of "technical information" as also pertaining to "about or relating to an individual".

2. The act of inferring personal information would appear to be activity in an attempt to identify or re-identify an individual without their consent. This should also be included in the threshold of "about an individual".

3. Extending the definition of "personal information" will benefit consumers, but should not be at a cost of unreasonably impeding societally beneficial uses of data (for example, for improved community health outcomes), or reducing incentives for regulated entities to deidentify consumer data for use and disclosure of effectively anonymised data. Amendments to the Act should address the standard required for data about individuals to be considered effectively anonymised and thereby outside the coverage of the Act. Some uses of effectively anonymised data should, however, be regulated by Australian Consumer Law or sector-specific statutes. This might include, for example, application of profiling to target unidentifiable individuals in ways that are unreasonable and contrary to legitimate expectations and interests of affected (unidentifiable) individuals.

4. Statutory penalties for malicious re-identification of de-identified data is welcomed and will strengthen the Act. It is important that any offence provisions only capture reidentification with intent to effect, or have the outcome of effecting, a harm to an individual. 'White hat' reidentification testing would thereby be excluded. The ability of privacy advocates to 'white hat' is an important safeguard against poor data governance by regulated entities. Unless the offence provisions are targeted in this way, there is a risk that entities will rely upon the availability of the offence as a substitute for assurance of effective anonymisation (deidentification).

5. The Act should apply to deceased individuals because identifiable deceased individuals can be a source of inferred personal information for living relatives of the deceased.

6. It is not clear how a request to stop the use of an individual's data would be consistent with the concept of a shared data right under Australia's consumer data right.

7. It is also not clear how an organisation could meet legal requirements to retain information for future law enforcement, given the statute of limitations does not expire for some crimes. We would recommend amending the wording on this.

8. The inclusion of 'personal information is sensitive information' as a sufficient reason for erasure request is somewhat odd and contrary to many public interest uses as it would put at risk all health databases, for example. A more nuanced take on that, perhaps with consideration for the anonymisation of data, would be a better fit.

Other notes

ACS members also offered clarifying notes on a number of other elements in the discussion paper, including the following:

1. Amendment 3.4 – to permit organisations to disclose personal information to state/territory authorities under an emergency declaration is very good, but the Act should caveat this by requiring the state/territory agencies to abide by agreed privacy principles with the information disclosed.

2. Amendment 10.4 – defining a secondary purpose – if this opens up potential for use of personal information for secondary purposes such as marketing, then it is unlikely to be a beneficial change for consumers.

3. Amendment 11.1 option 1 and amendment 13 – if adopted, this should include not just children, but also vulnerable adults (eg. adults with diminished psychological capacity). While the current amendment is titled 'children and vulnerable individuals', the text below it refers primarily to children, with references to parental involvement and age of the individual.

4. Amendment 24.7 – regarding a cost recovery levy to help fund OAIC's provision of guidance, advice and assessments. We question the purpose of this, given OAIC is already publicly funded to undertake these functions. Levying a cost may deter people from seeking OAIC's guidance and advice.

5. Small business exemption – small businesses are increasingly a vulnerable point of access for data related crime and with more online now, it is harder to justify an exemption from privacy provisions, especially through aggregation of multiple small businesses as targets. However, if the exemption is removed, additional support and free tools should be provided to assist with compliance with privacy principles, along with appropriately scaled penalties for noncompliance.

6. Pro-privacy default settings – whichever way this goes, it should ensure that the solution for consumers is clear. Presently, some businesses offer privacy settings that are unclear for consumers as to whether their selection is consistent with agreeing to access or with limiting access.

7. Provision 14.1, the withdrawal of consent to collect, use or disclose information; and Provision 15, the right to erasure of information – in circumstances where data collected is subsumed into to a larger dataset or into an algorithm used for delivery of a product/service, it may be near impossible for an entity to extract data related to an individual in order to comply with a directive to stop the ongoing use of that data or erasure of data. The wording of the Act should reflect the practical reality of the difficulty of those actions in certain circumstances.

Thank you again for you time and consideration. **<END>**