Submission to the Australian Attorney-General's Department in Response to the Privacy Act Review: Issues Paper

Dr Will Bateman (ANU), Dr Damian Clifford (ANU), Professor Seth Lazar (ANU)

Professor Kimberlee Weatherall (USyd)

On behalf of the Humanising Machine Intelligence Project, Australian National University

hmi.anu.edu.au

We are heartened that the Australian Attorney-General's Department has solicited submissions on the **Issues Paper** published on 30 October 2020 as part of the wider **Review** into the *Privacy Act 1988* (Cth).

Given the early stage of the Review, we have confined our detailed response to the Issues Paper to three main areas:

1. Scope and application of the *Privacy Act*: technological embedding;
2. The use of personal information: consent and other lawful grounds; and
3. Direct rights of action.

In **Annexure A**: we also provide shorter responses to some of the specific questions raised in the Issues Paper.

We would welcome the opportunity to continue engaging with the Review as it progresses.

1. Scope and application of the Privacy Act: Technological embedding

We submit that careful thought should be given to the current scope of the *Privacy* Act in light of evolving international practice regarding the legal protection of the human right to a private life.

The constitutional validity of the *Privacy Act* relies on Australia's binding international obligations under the *International Covenant on Civil and Political* Rights, particularly the obligation to protect the human "right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence". The right to privacy is understood as an enabling right in that the protection of privacy facilitates the enjoyment of many other human rights and values such as freedom of expression, non-discrimination, and individual autonomy. Hence, having an Act with an appropriate scope of application is key to the protection of one's privacy, but also enables the protection of many other important rights and interests.

The scope of the Act is in part defined by the information which it covers; we therefore welcome the discussion of the current definition of personal information (**Questions 2-5**). We believe that the correct approach is to align this definition to international best practice and to remove ambiguity by extending the scope to explicitly include device-related information in line with the Australian Competition and Consumer Commission's recommendation in the Digital Platforms report. That revised definition should include technical information (i.e. information that is not 'about' an individual but may still be used to single them out), and pseudonymous data. Both amendments respond to the practical realities of technological developments: as these data are regularly used to single individuals out.

We also welcome the Review's consideration of the complexities of "inferred data" as referred to in **Questions 3 and 36**. We believe that inferred data should be protected as personal and sensitive personal information, because the collection, use and disclosure of inferred information gives rise to the same risks of harm that arise from collection, use and disclosure of personal or sensitive

information in violation of the Australian Privacy Principles (**APPs**). In some cases there may be different or additional risks: for example, the inference may be wrong, but then used to make an important decision affecting the individual. We would welcome the opportunity to discuss our ongoing research on this topic.

The definition of personal and sensitive data is not the only important question of the scope of the Act. We submit that more detailed consideration should be given to whether the scope of the Privacy Act should more explicitly protect the entire lifecycle of data use as opposed to its current focus on collection and the purpose of collection. A switch in focus from the collection and the purposes of collection, to the 'fair processing' of personal information and the inclusion of certain additional protections such as a right to human review of automated processing, and to object to or restrict certain processing (as referred to again below) would more accurately reflect the significance of the protection of personal information in the digital age.

2. The use of personal information: Consent and other lawful grounds

The international best-practice regarding the human right to privacy requires two basic types of legal protections:

(i) personal information should only be collected or used with consent or another legitimate basis.
(ii) sensitive personal information should only be collected or used with explicit consent or legislation which provides a proportionate framework for collecting or using that information.

The current formulation of the APPs does not entirely reflect that basic approach to the legal protection of personal information.

APP 3.1-3.2 permits the collection of personal information by entities and organisations without consent if the information is, *inter alia*, "reasonably necessary for one or more of the [entity's/organisation's] functions or activities". APP 3.3 permits the collection of sensitive personal information without the need for explicit consent, with the same broad reference to "reasonable necessity" of entity's/organisation's "functions or activities", without clear indication of how those functions or activities are to be identified; whether those functions or activities are defined from an individual's perspective or the APP entity's, or whether those functions or activities need to be transparently set out by the entity/organisation. APP 6 permits very broad use and disclosure of personal (and sensitive) information, including use and disclosure without consent if "the individual would reasonably expect the APP entity to use or disclose the information" for a purpose which "is directly related to the primary purpose" for which the information was collected.

Those core parts of the *Privacy Act* provide a lower level of legal protection of the human right to a private life than the evolving international standards.

The Issues Paper invites responses on whether notice and consent are adequate tools to protect individuals' interests (**questions 20-22; 26-30**). We stress that two decades of research have shown that in the age of big data and AI these mechanisms may be necessary but are by no means sufficient. This is both because of notice-and-consent overload, and because the negative outcomes of data processing and analysis are not confined to only those who consent to their data being collected and processed.

If withholding consent makes no material difference to the consumer, given others' actions, then the giving of consent does not constitute genuine authorisation, but rather reflects the rational acknowledgment that individual choices cannot solve a collective action problem.

For notice and consent to be effective, they must be scaffolded by robust institutional assurances, so that consumers can trust that their digital safety does not depend on their unfailing vigilance and the vigilance of their fellow Australians. We would emphasise in particular the value of further discussion of these additional measures, now commonplace among our international comparators:

1. Privacy by design (using mathematically-proven cryptographic methods to protect personal information).
2. Data minimisation, including within that acknowledgment of the additional risks that arise from combining disparate datasets to yield insights that could not have been anticipated when user consent was initially sought.
3. Purpose limitation, including the right to object to some uses, and explicit legislation to prevent some uses (with or without consent). In general, the issues paper focuses quite narrowly on the collection of data, with less attention on its analysis and use. The latter, however, is where effects on consumers occur.

3. Direct rights of action: Individual rights

We welcome the Issue Paper's focus on the importance of direct rights to approach judicial bodies to obtain redress for breaches of the APPs (**Question 56**).

We agree that complicated issues arise in determining the trade-offs between (i) respecting rights to privacy and incentivising compliance with the Act and (ii) ensuring that court resources are not inappropriately diverted by trivial breaches. We do, however, note that many areas of law confer largely unfettered individual rights to approach courts for compensation, both as a matter of common law (contract, tort, property actions) and under statutory regimes including under the *Australian Competition and Consumer Act 2010* (Cth), the *Copyright Act 1968* (Cth) and the *Patents Act 1990* (Cth). The commercial and consumer rights protected by those legal regimes are no more important than the privacy rights enshrined in the ICCPR and protected in Australian law through the *Privacy Act*.

We submit that there are strong arguments in favour of providing direct access to judicial bodies for the enforcement of the APPs. One obvious justification is that providing direct rights to approach judicial bodies for full redress would obviate resource constraints currently experienced by the OIAC. But there are also principled reasons for extending direct rights of action, including:

(i) **where the APP entity is an agency**: respect for the strong constitutional principles guaranteeing access to judicial review of government action.
(ii) **where the APP entity is an organisation**: to create parity between enforcement of privacy law and other high-profile statutory legal regimes, such as copyright, patents and consumer protection law.

We also consider that an analysis of "open standing" provisions should be included by the Review. A number of prominent pieces of Australian legislation have open standing provisions and there is no obvious reason why such a provision could not also be included in an amended *Privacy Act*: eg *Competition and Consumer Act 2010* (Cth), s 80; *Environmental Planning and Assessment Act 1979* (NSW), s 9.45.

We also consider that careful thought should be given to conferring rights on individuals to receive compensation calculated on an "account of profits" basis: ie, by reference to the profit obtained by the collection or use of information obtained in contravention of the *Privacy Act*, rather than the quantification of harm suffered by such collection or use.

Annexure A: Shorter Responses

We offer the following shorter responses to some of the prompt questions; we would be very willing to elaborate on them in more depth in person.

Question 1: Should the objects outlined in Section 2A of the act be changed? If so, what changes should be made and why?
In the age of big data and AI, data protection regulation should aim at more than protecting individual privacy. The collection, aggregation and analysis of massive amounts of behavioural data exacerbates significant power asymmetries between people and the institutions that govern and influence their lives (whether states or digital platforms).

Question 4: Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?
At a minimum, there should be mathematically provable standards for what constitutes 'de-identification'. But we should also recognise that the power of big data derives from what can be done with it in the aggregate, which is largely unaffected even when the most rigorous differential privacy standards are used. If the goal of the privacy act is in part to respond to increasing concentrations of power caused by the collection, aggregation, and analysis of behavioural data by digital platforms, then deidentification is broadly immaterial. It is more important to explicitly limit the purposes for which such data can be used, or to more rigorously limit data collection in the first place.

Question 13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?
The Review should consider the degree to which advances in data collection and analysis techniques have enabled practices of workplace surveillance to bloom around the world and in Australia. Regulations intended to apply when digital communications were the exception, and most communication in a workplace would be offline, provide employers with extraordinary access to the lives of their employees now that many workplaces are almost entirely digital.

Question 36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?
The review rightly identifies that contemporary tools for aggregating and analysing data make it trivially easy to infer sensitive information (and personal information) on the basis of non-sensitive, non-personal information. As a result, it is effectively meaningless to classify information based on its content. It's also worth noting that sensitive information about a person X can be inferred based on some non-sensitive information about X, combined with much more information about millions of other people. In other words, the ability to infer sensitive information about X depends on collecting and analysing the behavioural data of many other people. Which again suggests the inadequacy of protecting data by appeal to notice and consent.

Question 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?
The idea of direct marketing is itself not quite adequate to capture the nature and role of online behavioural advertising. It is necessary to do a considerable amount of research both to update the act to address existing practices, and to determine whether and to what extent they can be consistent with protecting the autonomous decision-making of consumers.

Question 44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?
Data minimisation should be a general guiding principle for the Review, which would imply that retaining data on the promise of its subsequently becoming useful should be guarded against.