Submission to the TLRI Issues Paper – Review of Privacy Laws in Tasmania

Professor Margaret Otlowski, Director, Centre for Law and Genetics

Dr Lisa Eckstein, Adjunct Researcher

Emeritus Distinguished Professor Dianne Nicol

Thank you for the opportunity to provide input into this review process. In making this submission, we are drawing on our research expertise related to projects pursued through the Law Faculty's Centre for Law and Genetics including a recent project on Genomic Data Sharing. One of the areas focussed on for this research project has been on how genetic/genomic information and data is protected and implications for data sharing in the research context. We have also examined the changing status of genomic data and how laws deals with the ever increasing risk of re-identification of de-identified or even 'anonymous' information given the special status of genetic/genomic information.

An output from this project is a recently published paper, M Otlowski and L Eckstein, 'Sharing of Genomic Data: Exploring the Privacy Implications of the Changing Status of Genomic Data' (2023) 30 *Journal of Law and Medicine* 326. [redacted]

Because of the very particular lens of this privacy research (focusing on the protection of genetic/genomic data), this submission to the TLRI Issues Paper is deliberately limited in scope, providing responses to particular questions rather than a comprehensive response.

Question 2.4

Should the definition of 'personal information' be changed? Should it be consistent with the definition in the Privacy Act, or with the definition of personal data in the European Union's GDPR?

We see merit in making the definition in the Tasmanian *Personal Information Protection Act 2004* (Tas) as consistent as possible with the *Privacy Act 1988* (Cth). We note that Attorney General's Department *Privacy Act Review Report* 2022 (which because of timing issues, hadn't been considered for the Issues Paper) proposed an amendment arising from to replace 'about' in the definition of personal information (s6 *Privacy Act 1988* (Cth)) with 'relates to'. This would address the uncertainty following the *Grubb* decision as to whether technical information could be 'personal information' and better highlight that there needs to be a relationship between the information and the individual. This would also bring the definition closer in line with the European Union's GDPR.

Question 2.5

Are the other categories of information, including health and other forms of sensitive information suitable?

'Health information' is defined in s3 as including genetic information about an individual that is or may be predictive of the individual's or their descendant's health.

At paragraph 2.2.38 of the Issues Paper it is noted that unlike the first two descriptions in the definition of health information the description of genetic information does not include the terms 'personal information'. The Issues Paper goes on to comment that this creates some uncertainty as to the scope of the definition. It is worth noting in this context that this is also the case for the *Privacy Act 1988* (Cth) - it doesn't use the term 'personal information' in the definition of genetic information.

The definition of 'sensitive information' in the *Privacy Act 1988* (Cth) includes 'genetic information about an individual that is not otherwise health information'. We recommend we similarly expand the definition of 'sensitive information' in the *Personal Information Protection Act 2004* (Tas).

In the event that the definition of 'sensitive information' in the *Personal Information Protection Act 2004* (Tas) is amended to include genetic information, it would be important to keep abreast of the Attorney General's Department *Privacy Act Review Report* to amend the definition of 'sensitive information' in s6 *Privacy Act 1988* (Cth) to include 'genomic information,' and further, to amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act and clarify that sensitive information can be inferred from information which is not sensitive information (Rec 4.9). We recommend this approach also be adopted for the Tasmanian Act in the interests of consistency.

At page p12 of the Issues Paper there is a discussion about de-identification and pseudonymisation (paras 2.2.22-2.2.24) however there are no questions or proposed reforms in relation to this. The Attorney General's Department *Privacy Act Review Report* makes some important recommendations on this issue. Members of the Centre for Law and Genetics led by Dr Lisa Eckstein had made a submission on the earlier Attorney General's Department *Privacy Act Review* Discussion Paper which is acknowledged in the Report. (copy attached)

We recommend that we follow the lead of the Attorney General's Department *Privacy Act Review Report* recommendations on this topic to address uncertainties in the operation of the 'reasonable identifiability' test. Because of the integral role this test plays in the operation of the Act (only where a person is reasonably identifiable from the information will the information be treated as 'personal information' warranting protection) ambiguities in the application of this test is problematic.

To help address this the Attorney General's Department *Privacy Act Review Report* proposes a number of reforms to clarify when an individual will be reasonably identifiable from information by:

- introducing a list of factors to consider when determining whether an individual is reasonably identifiable; (Proposal 4.4)
- amending the definition of de-identify to make clear that whether information remains de-identified can change depending on the context ; (Proposal 4.5) and
- extending protections to de-identified information that are proportionate to the risk of the information being re-identified ; (Proposal 4.6). (Review Report, p 24)

Proposal 4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.

Proposal 4.6 Extend the following protections of the *Privacy Act* to de-identified information:

(a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information:
    (a) from misuse, interference and loss; and
    (b) from unauthorised re-identification, access, modification or disclosure.
(b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.
(c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.

These are, in our view, helpful suggestions which should be adopted also for the *Personal Information Protection Act 2004* (Tas).

Page 35 of the Issues Paper discusses 'fairness and reasonableness requirements' (focusing on recommendations of the Office of the Australian Information Commissioner.) This is conceptually linked with the 'fair and reasonable' test that has since been proposed by the Attorney General's Department *Privacy Act Review Report*:

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
(b) the kind, sensitivity and amount of personal information being collected, used or disclosed
(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency
(d) the risk of unjustified adverse impact or harm
(e) whether the impact on privacy is proportionate to the benefit
(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and
(g) the objects of the Act.

The Centre for Law and Genetics' submission made to the Attorney General's Department *Privacy Act Review, Discussion Paper* had supported the introduction of a fair use framework for the Commonwealth Privacy Act and we would similarly recommend that it be included in the reforms to the *Personal Information Protection Act 2004* (Tas).

Question 2.7

Should the PIPPs under the Tasmanian PIPA be amended to make them, as far as possible, consistent with the APPs in the Commonwealth Privacy Act as they currently exist or as amended in the future?

We see merit in consistency and they would then operate as intended.

Question 4.9

Should the Tasmanian Parliament legislate to introduce a statutory civil cause of action for interference with privacy in Tasmania in place of or in addition to existing legal protections? If so, how should this cause of action be framed, taking into account the matters of threshold and scope, breach, defences, and remedies?

The Centre for Law and Genetics' submission made to the Attorney General's Department *Privacy Act Review, Discussion Paper* supported the creation of a direct right of action under the *Privacy Act 1988* (Cth) available to any individual or group whose privacy has been interfered with by an APP entity, with remedies available as the court sees fit, including damages.

The Attorney General's Department *Privacy Act Review Report* includes a proposal for the introduction of a statutory tort for serious invasions of privacy a statutory tort for serious invasions of privacy in the form recommended by the ALRC Report 123 (Proposal 27.1). The Centre for Law and Genetics' submission to the Attorney General's Department *Privacy Act Review* Discussion Paper had also supported this proposal. Notably, the Report has recommended that this be done in consultation with the states and territories in the interests of ensuring a nationally consistent approach.

Australian Government Attorney General's Department Review of the *Privacy Act 1988* (Cth): Submission on Discussion Paper (October 2021)

Dr Lisa Eckstein[1], Professor Dianne Nicol[1], Professor Margaret Otlowski[1], Professor Ainsley Newson[2]

1. Centre for Law and Genetics, College of Arts, Law and Education, University of Tasmania
2. Faculty of Medicine and Health, Sydney School of Public Health, Sydney Health Ethics

We consent to this submission being published on the Attorney-General's Department website.

Dr Eckstein, Professor Nicol and Professor Otlowski acknowledge funding received under a Discovery Project Grant from the Australian Research Council (DP180100269)

Professor Newson acknowledges funding received from Australian Genomics. Australian Genomics is funded by the National Health and Medical Research Council (Grants GNT1113531 and GNT2000001) and the Australian Government's Medical Research Future Fund.

Thank you for the opportunity to provide comments on this Discussion Paper. Overall, we support the retention of a flexible, principles-based approach to privacy law, as well as enhanced transparency and complaint-handling mechanisms. Responses to specific proposals and questions are detailed below:

1. Objects of the Act

We support introduction of the concept of public interest in the objects of the Act. We recognise that it may take some time to fully explore the how this concept will apply in the context of the protection of privacy of individuals. However, there are many other instances where this concept has been appropriately employed in the protection of other individual interests (for example, in the protection of reputation).

2. Definition of Personal Information

2.1: We support changing the word 'about' in the definition of personal information to 'relates to', and agree that this promotes greater clarity, including in the context of genetic and genomic information.

2.2: We support the inclusion of a non-exhaustive list of the types of information capable of being covered by the definition of personal information. We also support the provision of a guidance that draws upon international case law and guidance, as well as a list of objective factors to help APP entities assess whether an individual is 'reasonably identifiable'. This will be of particular assistance in determining the reasonable identifiability of genetic and genomic information. We also suggest that a definition of genetic information be provided, e.g. to show that genomic information is synonymous, for the purposes of the Act, with genetic information. The terms 'data' and 'information' could also be distinguished.

2.3: We support defining 'reasonably identifiable' to cover circumstances in which an individual could be identified directly or indirectly and inclusion of a list of factors to support this assessment. Given the potential implications this definition change would have for research involving data linkage, clear information should be provided on how reasonability determinations should be made. It may be helpful to link this to undertakings made by researchers not to reidentify information, as is required, for example, under paragraph 3.3.22 of the *National Statement on Ethical Conduct in Human Research* ('Researchers receiving genomic information should not undertake nor permit attempts to re-identify the material or information or otherwise reduce the protection of the privacy of the participants.')

2.4: We support amending the definition of collection to include inferred or generated information, however, there is a need to ensure that legitimate research and clinical activities (for example, showing potential identifiability of online records, storing familial genomic records, etc) remain viable.

2.5 Requiring information to be anonymous before it is no longer protected by the *Privacy Act* could have significant implications for health and medical research, which relies on the retention of large amount of deidentified (but not anonymised) data: This data is retained by the original researchers, as a way of confirming data validity at a future time. It also can optimise the benefit of medical research for participants by allowing future contact, for example, if future analyses of the data show a clinically relevant finding. There also are increasing requirements for sharing deidentified data for future research. Providing raw, deidentified datasets is increasingly a condition of publication in high-impact medical journals (see, e.g., the statement by the International Committee of Medical Journal Editors on Data Sharing available here: http://icmje.org/recommendations/browse/publishing-and-editorial-issues/clinical-trial-registration.html). Internationally, bodies such as the National Human Genome Research Institute require the sharing of genomic data for all funded researchers (see https://www.genome.gov/about-nhgri/Policies-Guidance/Genomic-Data-Sharing/frequently-asked-questions/metadata-phenotypic-data-sharing). Bodies such as the Global Alliance for Genomics and Health are also strongly encouraging of international data sharing (see https://www.cell.com/cell-genomics/fulltext/S2666-979X(21)00036-7)

In any event, this proposal assumes that anonymisation is effective and will be irreversible. This has been established not to be true for at least certain kinds of genomic data, which means that this proposal rests on a false premise.

2.6 We support re-introducing the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

Further notes relating to proposal 2

We encourage particular attention to be given to the implications 'reasonable identifiability' for genomic information. We submit that there is a need to clarify more precisely when genomic information and data will fall within the scope of privacy laws, including the question of allocation to different types of genomic data (and samples) and how reasonable identifiability is to be understood in practice in relation to each. Additional guidance on the use of the data environment in the genomics context could also be beneficial.

We submit that the definition of sensitive information as it applies to genomic information warrants further consideration and guidance. One option might be to acknowledge the risk of re-identification even where attempts have been made to de-identify or anonymise that data.

9. Consent to the collection, use and disclosure of personal information

9.1 We have concerns about whether the proposed requirement for consent to be defined as being 'voluntary, informed, current, specific, and an unambiguous indication through clear action' would impede ethically acceptable research. It is also at odds with the *National Statement* and indeed existing practice and scholarly consensus, which is that forms of consent other than specific consent are acceptable in some instances. Genomic research, in particular, has moved towards models including broad consent for future research in many contexts (research with Indigenous peoples being the most common exception, where alternate forms of consent such as collective consent are also relevant). While it should remain an individual choice whether to agree to future data sharing, this option should be structured so as to facilitate various forms of consent. We encourage the amended Act not to unduly restrict consent to a very narrow individual-based, specific notion of consent. While not without issue, other forms of consent such as broad consent and collective consent are successfully used in many domains and have high participant trust.

10. Additional protections for collection, use and disclosure of personal information

10.1 We support a requirement that 'a collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances'. Moving towards a 'fair use' framework provides a more nuanced privacy environment than the current 'consent or anonymise' framework.

10.2 The proposed factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances appear appropriate.

25 A direct right of action

We support the creation of a direct right of action available to any individual or group whose privacy has been interfered with by an APP entity, with remedies available as the court sees fit, including damages.

26. A statutory tort of privacy

As some of us have already signalled in earlier submissions to the ALTC, we support option 1, the introduction of a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

Additional comments on the s 95/95A waivers under the Privacy Act

We wish to provide additional comments on the suitability of s 95/95A waivers under the *Privacy Act*. We support a clear mechanism to ensure that ethically acceptable research can proceed based on a waiver of consent. However, appointing Human Research Ethics Committees (HRECs) as the bodies to assess and authorise such a waiver warrants reconsideration. Although HRECs are well equipped to assess the respective risks and benefits of research (including research seeking a waiver of consent), they are not equipped

to act as ‘quasi-tribunals’, nor are they subject to judicial review or other forms of decision-making accountability. We suggest considering an alternative model such as the Confidentiality Advisory Group: a statutory body that operates in England and Wales to advise the Health Research Authority on the acceptability of access to personal information without consent for the purpose of medical research. We would be happy to provide additional detail on this should it be of benefit to the Department.