Kira White

From: Richard Griggs [redacted] >
Sent: Tuesday, 11 July 2023 8:06 AM
To: Law Reform
Subject: Review of Privacy Laws in Tasmania

To the Tasmanian Law Reform Institute

Thank you for the opportunity to provide this input into the review of privacy laws in Tasmania.

This submission focuses only on the Personal Information Protection Act 2004 (PIPA).

Since the PIPA was introduced 19 years ago in 2004 there has been a huge increase in the amount of personal data generated, with a corresponding increase in the need for that personal data to be stored securely and used appropriately. Harm can be done through inappropriate storage of personal information and this, I believe, is now much more widely understood within the community.

For detailed context and discussion regarding the expansion of data generation and increasing need for appropriate regulation, may I highly recommend "Net Privacy" (2020) by Sacha Molitorosz and "Privacy's Blueprint" (2018) by Woodrow Hartzog if they have not already been brought to your attention. For my book review of "Net Privacy" by Molitorosz, please see: https://tasmaniantimes.com/2020/06/net-privacy/

There is much that has changed since the introduction of PIPA which in turn means PIPA needs to change.

PIPA Section 4 - reform

The automatic override of PIPA by any "provision made by or under any other enactment" that is inconsistent needs to be reevaluated in light of the harms that can be done through loss or theft of personal information. I expect that it is accepted in 2023 that privacy protection has increased importance compared to 2004 and, as a result, PIPA should be elevated in the hierarchy of Tasmanian laws.

PIPA Principles - reform

PIPA operates by establishing a set of ten "Personal Information Protection Principles" (the "Principles") with which public authorities must comply.

I do not believe the Principles remain adequate and fit for purpose in 2023 and beyond given the rapid rate of technological change since the privacy laws were enacted.

For example, principle 4(2) requires that a personal information custodian must "take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure.". I expect both public sentiment and good privacy practice now requires that to be expanded by requiring a public information custodian to notify individuals when there is in fact misuse, loss, unauthorised access, modification or disclosure (all referred to in my submission as "data breach"). These damage that can be done from data breach is understood and mandatory disclosure to impacted individuals should be required by law. For mandatory disclosure to be meaningful, the disclosure needs to contain practical and useful information that can be understood and acted upon by the individual.

For a further example, principle 4(2) requires that a personal information custodian "must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose." I expect that public sentiment and good privacy practice to now have superseded this obligation to take "reasonable steps" and instead have a mandatory and binding obligation to destroy personal information that is no longer needed.

"authorised or required by law" - area for reform

Privacy Principle Number 1 states that a pubic authority may only collect personal information relevant to one of its functions or activities. This is an important limitation and ensures that public authorities are only collecting personal information that is relevant to their functions or activities.

In addition to Principle Number 1, PIPA enables public information custodians to collect, use or disclose personal information where “authorised or required by law”. This set of words features five separate times in PIPA

In effect, the “authorised by law” sections can be used as a mechanism by government to add to its own functions or activities and change and expand what they are authorised to do with the personal information.

Seen in this light, the ‘authorised by law’ section can operate as an exemption mechanism under which government can dramatically expand the uses to which it can deploy personal information, regardless of what the reason for collecting the information was to begin with.

In recent years it has emerged that, on occasion, this ‘authorised by law’ mechanism is being activated by the State Government by writing *regulations* instead of *legislation*. For example, the transfer of Tasmanian drivers licence photos to a national facial recognition scheme was authorised by a 2017 amendment to the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010.*

The relevant amendment regulations were the *Traffic (Driver Licensing and Vehicle Registration) Amendment (Identify Matching Services) Regulations 2017*.

I doubt that this was what was intended in 2004 when the reference to ‘law’ was used in PIPA. Instead, and consistent with the objective of full transparency, I suggest the original drafters and parliamentarians intended this reference to instead be read as a reference to an Act of Parliament, passed after public debate and parliamentary scrutiny on the floor of both houses of State Parliament.

Regulations are examined by the Subordinate Legislation Committee, however this process is much less transparent than the process of State Parliament examining legislation. For example, generally no records are available of the deliberations of the Subordinate Legislation Committee, no public report is issued by them, nor is public consultation undertaken as a general rule.

In the interests of transparency, this needs to be rectified and the “authorised by law” sections should be amended to be clear that law does indeed mean a law passed by State Parliament.

To give context to the magnitude and scale of personal information that can be dealt with via regulations, it is worth noting that the transfer of 468, 392 Tasmanian drivers licence photos to a national facial recognition scheme occurred:

a. Without consent of individuals concerned

b. Without express approval from State Parliament as a whole.

c. With the approval of the Subordinate Legislation Committee who examined the 2017 Amendment Regulation authorising the transfer. The Committee met in private, did not seek public submissions and no public report is available on its deliberations

d. In the absence of Commonwealth legislation or regulate the operation of the national facial recognitions scheme or provide.

sections 13 and 14 - area of reform

In addition to the ‘authorised by law’ process, a further exemption mechanism exists in sections 13 and 14 of the privacy law.

Section 13 states that:

"(1) A personal information custodian may apply to the Minister for an exemption from compliance with any or all provisions of this Act.

(2) An application is to –

1. (a) specify the provision or provisions to which the application relates; and
2. (b) specify the information or class or classes of information to which the application

   relates; and

3. (c) specify the personal information custodian or custodians or class or classes of

   personal information custodians to which the application applies; and

4. (d) specify the reasons for the exemption; and
5. (e) specify any public benefit involved; and
   (f) specify any relevant law, code of practice or other instrument under which it proposes to operate; and
   (g) include any other information the Minister determines."

Section 14 then permits the Minister to approve an application

On 25 November 2020 an exemption was gazetted in the Tasmanian Government Gazette. The exemption applies to any information that "has the potential to be relevant to an actual or potential civil claim against the State of Tasmania". The exemption applies to eight separate departments.

There are several problems with the exemption process allowed for under sections 13 and 14 and the process to be followed by the Attorney General. These problems centre on the fact that the process:

1. amounts to government applying to itself to be exempted from legal obligations that would otherwise apply

2. does not involve the public in any way with the public only being notified after the decision has been made by way of the government gazette

3. does not include any requirement to gather views and information from the Tasmanian Ombudsman, who has oversight of the privacy laws

4. does not provide for the public to seek a review of the decision. It is worth noting by comparison that a decision of the Anti-Discrimination Commissioner to grant an exemption from compliance with the Anti-Discrimination Act is reviewable (section 59).

In light of the extensive suite of specific exemptions already provided for under PIPA(see section 7 to 12), it does not appear reasonable or necessary for the government to have a 'back stop' exemption that allows it to simply and easily exempt itself from compliance at its own election. Sections 13 and 14 should be repealed.

Thank you again for this opportunity to provide input into the review.

regards

Richard Griggs