Submission: Tasmania Law Reform Institute, *Review of Privacy Laws in Tasmania* Issues Paper No. 32.

Submitted by the Hon. Meg Webb MLC
Independent Member for Nelson

21 July 2023

Introduction

The thorough research and work undertaken by the Tasmania Law Reform Institute (TLRI) in the production of the *Review of Privacy Laws in Tasmania*, Issues Paper No. 32, is to be commended. I welcome the opportunity to make a submission to this comprehensive review.

> **At the outset I am happy to indicate I consent to the TLRI regarding this submission as a public submission, and the TLRI may refer to or quote directly from my submission and name me as the source of the submission in relevant publications.**

As noted in the Issues Paper, this brief was first accepted by the TLRI in December 2019. Since that date we have experienced the almost two years of the COVID-19 Pandemic State of Emergency period, and its related disruptions. On one hand those disruptions may have been frustrating when it came to progressing this important review, however on the other hand that extended period of time has provided a range of other privacy matters to become apparent, which can now also be considered by this Review.

I note with particular interest the Issues Paper's assessment that despite providing Tasmania's primary privacy framework, the *Personal Information Protection Act 2004* (Tas) ('PIPA') contains, "*… multiple gaps in its scope, operation, and enforcement that can jeopardise privacy*." [1]

Further, that currently, *"…there is no comprehensive privacy regulation in Tasmania. Rather, privacy protection is fragmented across different laws that protect different types of privacy in different specific circumstances.*"[2]

That formal assessment in itself vindicates the current terms of reference set for the TLRI and this review. In light of the modern and fast-evolving digital and technological landscape, it is also cause for serious concern and injects considerable urgency into the current public debate.

Structure and Scope of Submission

This submission consists of two main parts: the first of which provides some initial general commentary on specific examples of privacy concerns. Part Two then focuses upon the 26 questions posited in the Issues Paper.

As noted by the Issues Paper, coinciding with the TLRI state-based inquiry, the Commonwealth Attorney-General has also been undertaking a review of the federal *Privacy Act 1988* (Cth). The Commonwealth *Privacy*

[1] Tasmania Law Reform Institute, *Review of Privacy Laws in Tasmania* (Issues Paper No 32, March 2023) printed hardcopy version; pg xii.
Note: page numbers differ between the hardcopy printed booklet version of Issues Paper No. 32 and the online digital version. Unless otherwise specified all in-text citations refer to the hardcopy version of the Issues Paper No. 32.
[2] Ibid: pg xii.

Act Review Report was released in February 2023, with feedback sought on the government's response to that report over the following month.

This submission has also been informed where applicable to the current state discussion by a range of published submissions made to that federal review process.

Finally, this submission does not seek to replicate the detail or legislative analysis as already compiled in the Issues Paper. Instead, where appliable, it will provide supporting information and actual lived examples derived from reports on privacy concerns arising during the COVID-19 pandemic, and following revelations of Tasmania's involvement in the proposed national Facial Recognition Drivers Licence Scheme.

PART 1: GENERAL COMMENTARY

Human Rights Framework Needed

As mentioned above, the TLRI Privacy Laws Review Issues Paper describes the current status of Tasmania's privacy laws and protections as "*fragmented across different laws,"* and providing a "*fragmented landscape*" of safeguards.

This echoes a similar assessment of an earlier TLRI Inquiry in 2007 on the question whether Tasmania requires a Charter of Human Rights. When launching the Final Report of that review, the TLRI media release of the time stated:

> "*In Tasmania, a patchwork of sources provide protection of human rights, including the Tasmanian and Australian constitutions, international law, common law and state and federal laws. However, the protections offered by these sources are fragmented and incomplete – working out what rights are protected, when and how, is a complex task*."[3]

Highlighted by United Nations' conventions such as the *International Convention on Civil and Political Rights*, to which Australia is a signatory, it is worth noting there is a clear and natural synergy between the need for legislative human rights protections as well as strengthened and comprehensive privacy and personal information protections.

In fact, one of the specific rights recommended by the TLRI for inclusion in the proposed Tasmanian Charter of Rights was the "*right to privacy and reputation*."[4]

For example, a common element and theme shared across both privacy and human rights' frameworks public debates is the definitions of "privacy" and "personal information", for example. Another common theme of discussion is the issue of enforceability of any protections put into place.

While I recognize it may be beyond the scope of the current TLRI Privacy Law Reform inquiry to consider or make specific recommendations regarding the absence of a legislated human rights framework at either the federal or state level, it is important to note how the two are fundamentally interlinked and the implications of the absence of a formal Human Rights legislated framework.

Specifically, history has shown us that technology has a habit of outstripping policy development, regulation, and legislative redress. This is a key challenge facing the current review of the state's privacy laws – it not only has to consider how best to plug the current identified gaps and propose how the state can catch-up, as it were, the Review is also expected to look ahead as much as possible and anticipate "emerging" relevant

[3] TLRI Media Release, 12 October 2007, *Charter of Rights Recommended for Tasmania*.
[4] TLRI, October 2007, *A Charter of Rights for Tasmania*, Report No. 10 (online); pg 2.

laws and obligations, as well as potential needs of individuals in an acknowledged "evolving technological environment".[5]

Hence, a legislated Tasmanian Human Rights Charter could provide a consistent reference point of fundamental principles and criteria to be applied consistently when evaluating potential impacts of technological development and policy responses, despite individual pieces of legislation becoming ineffectual or out of date in some way over time.

This intrinsic synergy between an effective legislated and enforceable human rights framework and effective privacy protections was also identified by the Australian Privacy Foundation in a formal brief provided in 2018 to the UN Special Rapporteur on Right to Privacy, Professor Joseph Cannataci. That brief identified as systemic issues of concern as including:

> *"[the] absence of comprehensive constitutional protection of human rights, no cause of action for serious invasions of privacy (ie a privacy tort), narrow definitions of 'personal information' and significant exemptions to the Privacy Act 1988 (Cth), and a captive and underfunded regulator."*[6]

Further:

> *"Currently in Australia there is no comprehensive constitutional protection of the general rights of citizens or a charter of human rights at the federal level, which leaves citizens vulnerable to human rights infringements by both the state and other citizens."*[7]

After providing a range of examples detailing instances where infringements upon citizen privacy and personal information have incurred, including the commonwealth scheme commonly referred to as 'RoboDebt' the Brief includes six main recommendations which reinforce the interrelationship of human rights and privacy protection:

1. Introduce an enforceable charter or bill of human rights at the federal level;
2. Introduce a privacy tort;
3. Appoint a Federal Privacy Commissioner and increase funding to the Office of the Australian Information Commission;
4. Implement proactive principles of privacy by design and data protection by design and default rather than reactive remedial attempt;
5. Consider the impacts of data collection and use in ways that extend beyond privacy, and;
6. Encourage, respect and promote Indigenous Data Sovereignty initiatives and associated principles in the collection and use of information concerning Australia's Indigenous Peoples.[8]

Additional to its emphasis upon the need for a rigorous human rights framework in which to imbed privacy protections, the Australian Privacy Foundation's 2018 Brief also serve to highlight that the potential risk to citizens' privacy and personal information rights can be, and has been, from government authorities as much as private 'bad actors'.

This can pose a considerable challenge for meaningful privacy law reforms as regulatory gaps, oversights or ineffectual measures as identified by civil society may be perceived by government authorities as

[5] TLRI Issues Paper No 32, March 2023: pg. x.
[6] Australian Privacy Foundation, 15 August 2018: pg. 2.
[7] Ibid: pg. 3.
[8] Ibid: pg. 2.

opportunities instead – resulting in civil society and the state being in conflict and potentially infringement of individuals' or marginalised communities' human rights being rationalized and downgraded.

While it is not unusual for there to be tension between civil society and the state over a range of policy matters, it is arguable that the absence of an enforceable Tasmanian human rights framework against which state laws and regulations are evaluated exacerbates those tensions, while also contributing to the current fragmentation of privacy protections as assessed by the TLRI.

Facial Recognition Technology

The National Driver Licence Facial Recognition Solution (NDLFRS)

A catalyst for seeking a referral of this privacy law reform review terms of reference to the TLRI was the discovery that in December 2018, thousands of Tasmanian drivers licence photos were transferred to the National Driver Licence Facial Recognition Solution (the NDLFRS), despite the lack of any Commonwealth legislation providing necessary oversight and privacy protections.

The Tasmanian State Parliament oversight mechanisms at the time were also minimal as the transfer of this considerable number of Tasmanians' personal data occurred via regulation only. This regulation process does not automatically involve broader public debate or consideration by the entire State Parliament, and in this instance was assessed by the Subordinate Legislation Committee as regulations only. Although the Committee can call for public submissions, it did not choose to do so for these particular regulations and nor is there any publicly available report of the Committee's deliberations.

Section 2.2.47 of the Issues Paper provides a brief summary of the current hiatus of the actual activation of the NDLFRS in the ongoing absence of Commonwealth oversight legislation being passed by the federal parliament.

Despite the national *Identity-matching Services Bill 2018* being re-introduced as the *Identity-matching Services Bill 2019* in the federal parliament on the 31st of July 2019, it lapsed on the dissolution of that parliament in April 2022. In the interim it was also subject to two federal parliamentary committee inquiries: the Parliamentary Joint Committee on Intelligence and Security in August 2019 and the Parliamentary Joint Committee on Human Rights in 2018.[9]

Recommendation 1 of the the Federal Parliamentary Joint Committee on Intelligence and Security report into *Identity-matching Services Bill 2019* states:

> 5.7 The Committee recommends that the Identity-matching Services Bill 2019 be re-drafted taking into account the following principles:
>
> - the regime should be built around privacy, transparency and subject to robust safeguards,
> - the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality,
> - the regime should be one that requires annual reporting on the use of the identity-matching services, and
> - the primary legislation should specifically require that there is a Participation Agreement that sets out the obligations of all parties participating in the identity-matching services in detail.
>
> The *Identity-matching Services Bill 2019* should be re-drafted taking into account the Committee's findings in this report. The Committee notes that the findings alone do not set out

[9] The Human Rights Parliamentary Committee first examined the initial *Identity-matching Services Bill 2018* and therefore did not re-examine when the same Bill was reintroduced in 2019.

all of the matters that would bring the Identity-matching Services Bill 2019 into line with the principles outlined above.[10]

The federal Parliamentary Joint Committee on Human Rights found:

> *"In relation to this measure [the NDLFRS], the committee concluded that there was a risk of incompatibility with the right to privacy through the use of the existing laws as a basis for authorising the collection, use, disclosure and retention of facial images. The committee stated that setting funding for the Capability without new primary legislation which circumscribes the Capability's operation raises serious concerns as to the adequacy of safeguards to ensure that the measure is a proportionate limitation on the right to privacy."*[11]

The Committee report continues by raising concerns over adequacy of the proposed Bill's safeguards to govern the collation, storage and use of facial images and other biometric data, compliance with international human rights law, and whether any limitations imposed on the right to privacy are proportionate.

Yet, as mentioned above, at the state level, and despite the lapsed state of the necessary Commonwealth legislative framework, it emerged during Government Business Scrutiny hearings held in December 2019 that the Tasmanian government proceeded in 2018 with the collation and provision of Tasmanians' photographic and personal information for the specific purpose of the application of controversial facial recognition technology.

Exacerbating community concern and outrage at the time the transferal of Tasmanians' drivers licence data became public was the confusing, lacking in detail, and occasionally conflicting information provided by the state government. For example, initially it was unclear exactly how many Tasmanians' drivers licence photos had been supplied. Initially it was reported 410, 000 Tasmanian licence photos had been supplied, whereas in March 2020 it was confirmed that the National Driver Licence Facial Recognition Solutions held 430, 113 Tasmanian licences.[12]

More recently, via the Tasmanian Legislative Council questioning process,[13] government data details that a total of 468, 392 Tasmanian drivers licence photos were transferred to the NDLFRS between December 2018 and the 16th of December 2020 when the transfer of records was paused.

Further, following the public outcry at the time, a statement from the State Minister for Infrastructure and Transport dated the 28th of October 2020 declared the Tasmanian data transferred to the NDLFRS will not be used until both Commonwealth legislation is in and relevant Tasmanian legislation reviewed, with the latter to occur in context of any eventual Commonwealth legislation.

While the temporary suspension of the transferal of Tasmanian data to the NDLFRS may offer a degree of reassurance for the community, it also serves to highlight serious concerns with the state decision-making process particularly regarding potential adverse impacts upon citizens' right to privacy. For example, the temporary suspension is an acknowledgment – a belated one - that reliance solely upon using state regulations as an authorizing mechanism is inadequate, and that the state's *Personal Information Protection Act 2004* may also not be adequate for this particular purpose. These concerns should have been identified, evaluated and acted upon prior to any transfer of Tasmania's photographic data for future facial recognition technological application.

---

[10] Parliamentary Joint Committee on Intelligence and Security, October 2019: pg. iii.

[11] Parliamentary Joint Committee on Human Rights, June 2018, *Report 5 of 2018*: pgs 109-110.
Note: the Committee did not re-evaluate the re-introduced 2019 Bill as it did not differ from the 2018 version, hence the Committee's earlier critique stands.

[12] Senate Standing Committee on Legal and Constitutional Affairs Additional Estimates, March 2020 – answer provided data current as at 18 March 2020.

[13] A collation of Questions put by the Hon. Meg Webb MLC and responded to by the government is provided in Appendix 1 of this submission.

The case-study of the transferal of Tasmanian data to the NDLFRS highlights significant points of concern relevant to this Privacy Laws Review more broadly, including the following matters:

- The role of informed and active consent (as opposed to presumed and passive consent);
- The need for strong privacy protections and oversight safeguards not only in place but also understood by those surveilling as well as those surveilled;
- The need for regular and rigorous auditing of those protections and safeguards to ensure they are fit for purpose;
- Issue of proportionality.

Ironically, it is worth pointing out, that the NDLFRS' current implementation limbo is not due to the application of a rigorous human rights and privacy protection framework, but the absence of such a fundamental legislative regime. Clearly this is a perverse outcome under our parliamentary democratic system, and does little to provide public confidence in our system of governance at either national or subnational level.

Government Proposal to use Facial Recognition Technology in Gaming Venues

In January 2022 the Treasurer and Minister for Finance issued a Ministerial Directive to the the Tasmanian Liquor and Gaming Commission (TLGC) to investigate the extent to which facial recognition technology (FRT) and player card gaming for electronic gaming machines in casinos, hotels and clubs could minimise gambling harm.[14]

The TLGC undertook a stakeholder consultation process involving both face-to-face sessions and a submission process, to which 49 written submissions were received.

The TLGC's Report to the Treasurer, released on 15th of September 2022 (although the report itself is dated June 2022), states, "*The Commission does not recommend implementation of FRT as it is not an effective tool for wider prevention of harm in gaming venues in Tasmania*." [15]

The report cites concerns over inaccuracy of Facial Recognition Technology including potential impact upon quality of control images, quality of venue devices, use of algorithms to mention a few considerations. Concerns arising in the consultation process, particularly from civil society and community organisations, were acknowledged, including the implementation of FRT, specifically concerning the privacy considerations, regulatory and training requirements, the current exclusion scheme amendments and evaluation.[16]

The TLGC concludes by stating:

> *"Broadly, the use of FRT is contentious. Consideration will need to be given as to whether there is a need to amend, or introduce, legislation that regulates the use of excluded persons' data with the operation of FRT in Tasmania which must have adequate consumer protections and comply with the Australian Privacy Principles (Commonwealth), the Personal Information Protection Principles (Tasmania), the Australian Human Rights Commission's Human Rights and Technology Final Report (2021) and any other relevant legislation. The Commission notes that the South Australian legislation and licence conditions to introduce FRT predate the delivery of the AHRC's Final Report."*[17]

[14] Tasmanian Government Gazette, 26 January 2022; pg 59.

[15] TLGC, June 2022, *Investigation of harm minimisation technologies: facial recognition and player card gaming Report to the Treasurer*: pg 8.

[16] Ibid: pg 19.

[17] Ibid: pg 24.

The Tasmanian Government's formal response to the TLGC Report regarding the possible implementation of Facial Recognition Technology includes an acceptance of the latter's view that, "*… FRT is not an effective tool for wider prevention of harm in gaming venues (other than identifying already excluded persons).*"[18]

The purpose for raising this particular matter within the context of this Privacy law Review is that it provides an example of a potentially ad hoc and piecemeal approach by government to utilising various forms of facial recognition technology in the pursuit of particular areas of public policy, despite the absence of a comprehensive human-rights sensitive rigorous regulatory framework, or protections and oversight mechanisms.

Private Sector use of Facial Recognition Technology

In June 2022 Australian consumer advocacy group CHOICE revealed the national retailers Bunnings, the Good Guys and Kmart were employing facial recognition technology to capture the biometric data of customers accessing their stores.

While Good Guys suspended its use of the facial recognition technology following the CHOICE revelations, the Office of the Australian Information Commissioner (OAIC) announced on the 12 July 2022 it had opened investigations into the personal information handling practices of Bunnings Group Limited and Kmart Australia Limited.[19]

However, in July this year CHOICE published subsequent research identifying the use of facial recognition technology across sporting and entertainment venues, including major stadiums.[20]

The CHOICE study analysed 10 major Australian stadiums and stadium operators' conditions of entry publications and privacy policies, and found that many provided for the use of facial recognition technology to collect biometric information yet were "vague or non-response" when further information was sought.

Alarmingly, it appears from the venue survey undertaken by the researchers that people purchasing a ticket for an event is then interpreted as providing consent for the collection and use of their biometric data. CHOICE provides the Melbourne Cricket Ground's (MCG) conditions of entry as stating:

> *"Patrons consent to the collection of biometric information (including biometric templates) for what is reasonably necessary for one of the MCG's functions or activities".*[21]

According to CHOICE the MCG failed to respond to requests for clarification on type of data collected, its use, storage and length of time it is stored. Of further concern is that those venues and operators who did respond to queries were reportedly 'vague' when it came to similar data types, purposes for collection, and timeframes by which data was kept.

Additionally, serious privacy concerns regarding facial recognition technology capturing indiscriminately biometric data of minors were raised by a cited University of Technology Sydney (UTS) Human Technology Institute researcher:

> *"We're talking here about semi-public places where community members, including a lot of children, gather and watch sports events and entertainment. In this context, the risks of using*

[18] *Tasmanian Government response to the Tasmanian Liquor and Gaming Commission's Report to the Treasurer on its Investigation of harm minimisation technologies: facial recognition and player card gaming*, September 2022: pg. 33.

[19] OAIC, 12 July 2022, "OAIC opens investigations into Bunnings and Kmart", viewed at https://www.oaic.gov.au/newsroom/oaic-opens-investigations-into-bunnings-and-kmart on 10 July 2023.

[20] See CHOICE website article, *"Facial recognition technology in use at major Australian stadiums"* published 5 July 2023: https://www.choice.com.au/frtstadiums, viewed 19 July 2023.

[21] CHOICE website article, 5 July 2023: https://www.choice.com.au/frtstadiums, viewed 19 July 2023.

surveillance technologies to our civil and human rights really appear to outweigh any benefits to the sorts of security incidents you'd potentially be seeing at an event like a sporting match." [22]

The private sector examples of biometric data collection identified by these CHOICE investigations also highlight a trend of reversing the onus of responsibility onto the consumer.

In these examples, the retail outlets and venue operators involved presume that a minimalist and easily-overlooked disclaimer in the small print of tickets or access points of buildings stating some form of facial recognition technology is in use, equates the customer providing informed consent.

Somehow, potential customers are meant to presume this technology will be potentially capturing their sensitive biometric data, that they should proactively search for such disclaimers before entering the local outlet of a national retailer, or purchase a general admission ticket to a sporting event or concert, and then to decide not to proceed seeking access to these semi-public places should they decide they do not want their sensitive biometric data to be collected, stored and used for undefined purposes over an equally undefined period of time.

This presumed reversal of onus of responsibility demonstrates a highly unsatisfactory and deeply worrying power-imbalance between those with the means to surveil and those potentially being surveilled.

It is arguable there is a similar assumption behind the Tasmanian government's quiet handing over of more than 430, 000 Tasmanians' drivers licence photos – that those citizens by engaging in the voluntary provision of personal identifying information as part of the legal and social contract entered into for the purpose of obtaining authorization to drive a vehicle on public roads have also, by default, provided consent for that sensitive biometric data to be provided to another jurisdiction for a different purpose.

Another shared assumption between these scenarios is that the only apparent option by which an aware citizen could consciously withhold consent is by choosing to go without – to choose to not apply for a legal driver's licence, or to choose to not seek to access a semi-public space operating as a retail outlet or entertainment venue.

This assumption of a reversal of responsibility to inform which appears to manifest in both the private and public sectors, according to these examples cited above, highlight key critical aspects pertinent to this privacy law review, including:

- The meaning of informed consent;
- The presumed shared understanding between authorities/private sector and individuals that to engage in standard social activities is to accept as default a degree of voluntary relinquishment of the right to privacy, and proportionality of that impact;
- The use, storage, transferal to other entities, and duration of storage of sensitive and personal data;
- Capacity to opt in and opt out;
- Extent of auto-data collection, automated decision-making and potential for profiling;
- Gaps between consumer laws and privacy laws;
- Oversight and enforcement of regulatory frameworks.

[22] Lauren Perry UTS Human Technology Institute cited in CHOICE website article, 5 July 2023 https://www.choice.com.au/frtstadiums, viewed 19 July 2023.

Other Examples of Private Sector use of Personal Information Provided

There are other examples of private enterprises appropriating personal information volunteered by clients and customers and seeking to use that information for purposes, such as monetizing it, other than that for which it was provided.

During the COVID-19 pandemic and as part of the Tasmanian social distancing regime, it was asserted by the state – and arguably accepted by the majority of the community – that means of contact tracing individuals' movements when accessing semi-public and public spaces needed to be put into place for public health reasons. Hence check-in requirements were gazetted via a direction issued by the Director of Public Health on 18 March 2021, where people were required either via the digital COVID Check-In TAS App, Q-codes, or manual hand-written log-in sheets to volunteer basic personal identification and contact information.

While still warranting public scrutiny as a public policy position, the rationale and premise was that for the 'greater good' and for a temporary – but still undefined at the time – period there was a public health need to impact citizens' rights to privacy and freedom of movement. As such it is arguable this pandemic-related public health policy met a proportionality test on its impact upon privacy rights.

Further, the information provided by the government at the time detailed that:

> *"the information provided through the Check in TAS App is collected for the purposes of managing the threat to public health posed by COVID-19. The information is only disclosed for the management, detection, notification, treatment or prevention of COVID-19 as authorised under the Public Health Act 1997."*[23]

Further, any information collected via the App would be deleted automatically after 28 days.

However, some businesses and venues used hand-written log-ins, particularly while the App was being rolled out, and as an acknowledgement that not all customers had mobile phones capable of using the digital check-in options.

During this time, there were reported instances – including cases which I personally raised – of people abiding by the public health required check-in formalities at either Tasmanian retail and/or hospitality venues to then subsequently be targeted with marketing advertising from those venues and businesses.

There was a clear and major oversight by the authorities to provide relevant information and training regarding privacy and personal information management responsibilities along with pandemic contact tracing measures.

It became quickly apparent at the time that clarification was required that personal information "volunteered" in compliance with a public health directive, was not carte-blanche consent for that information to be used by those businesses and venues for other purposes.

Although the personal data obtained in the above scenarios described do not necessarily include biometric data or the use of facial recognition technology, it does illustrate yet again when an ostensibly "for the greater good" collection of individuals' personal information can be accidentally or deliberately exploited for other purposes, particularly in the absence of a rigorous legislated protections and oversight framework.

[23] Department of Premier and Cabinet (DPAC) website, "Required use of Check-in TAS App - Policy and FAQs" March 2021: https://www.dpac.tas.gov.au/divisions/ssmo/coronavirus/required_use_of_check_in_tas_app_policy_and_faqs

PART 2: TLRI PROVIDED CONSULTATION QUESTIONS

It is worthwhile noting that this Review of Tasmania's Privacy Laws is occurring at the time a similar review is being undertaken by the federal Attorney-General of the Commonwealth *Privacy Act 1988*. In response to the latter review there have been calls for the development of national model privacy legislation particularly in regards to the use of facial recognition technology.

This submission supports the investigation and potential development of model legislation driven by the right to privacy at its core, due to the fact that recent government forays into utilising facial recognition technology, for example, has involved cross-jurisdictional mechanisms and intent. While this submission recognises it is beyond the scope of the TLRI Review to develop national model legislation, the responses provided below to the set consultation questions are informed to some extent by awareness that elements potentially impacting Tasmanians' privacy do so due to their potential application in other jurisdictions, such as the proposed national drivers licence database.

It is beyond the scope of this submission to provide detailed responses to all the set consultation questions, and instead indicative and in-principle responses will be provided.

Chapter 2—Privacy protection: Scope and application of the PIPA

Question 2.1

Are there Tasmanian public sector agencies or organisations not sufficiently covered by the PIPA, or which should otherwise be included in the definition of 'personal information custodian'?

As identified in the Issues Paper No. 32 there are certain public bodies currently exempt from the PIPA including courts and tribunals, the Solicitor-General and employees, the DPP and employees.

It is arguable that all public sector agencies, including those currently exempt, should be subject to the PIPA and defined as 'personal information custodian', as the default position. If necessary, provision could be made under the Act for courts and tribunals and other public legal officers and employees to have access to exemptions when supported by a public interest test.

Question 2.2

Should non-government organisations, such as for-profit businesses, charities, or political parties registered in Tasmania, be subject to privacy regulation in addition to any obligations under the Privacy Act?

Yes. Any government or non-government organisation which is in a position of obtaining either basic personal information or sensitive information, such as potential biometric data collection via surveillance mechanisms for entering premises etc, should be subject to privacy regulation.

Question 2.3

To what extent are government contractors appropriately subject to obligations under the PIPA? Should there be additional obligations on Tasmanian government agencies entering into contracts with private bodies to ensure that privacy obligations are able to be enforced against the contractor?

Government contractors can be a potential 'loop-hole' in context of consistent and rigorous application of privacy protections. There does need to be clear and reportable additional obligations on Tasmanian government agencies entering into contracts with private bodies to ensure that privacy obligations are able to be enforced against the contractor.

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?

The current definition of 'personal information' should be amended to be consistent with the definition of personal data in the European Union's GDPR which defines personal information with a broader scope.

Question 2.5

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

The current range of options and flexibility provided by the PIPA for health information (such as options to disclose health information on behalf of individuals unable to provide or communicate consent may be practical, on the proviso there is also adequate, appropriate and sufficient oversight and reporting of any application of those options.

However biometric information should be included as recognised as a discreet form of 'sensitive information' under the PIPA. As should genetic information that is distinct from an individual's health information, as per the Commonwealth Privacy Act's provisions.

Question 2.6

Are the exceptions, including the process for declaring and publishing public benefit exemptions, suitable?

No, the current public benefit exemption provisions are inadequate. As a minimum the oversight provisions of Ministerial determinations should be boosted to include the requirement that any such determination is to be a parliamentary disallowable motion, as is the case in Queensland, NSW and Victoria.

Additionally, there needs to be a searchable register of public interest determinations maintained.

Chapter 2—Privacy protection: Personal Information Protection Principles

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?

Yes, the PIPPs under the Tasmanian PIPA should be amended to make them, as far as possible, consistent with the Commonwealth Privacy Act's APPs as they currently exist or as amended in the future.

Question 2.8

Are there any other amendments to the PIPPs that you think should be made?

These considerations maybe covered by 2.7's recommendation to amend the PIPPS to be as consistent with the APPs as possible, but it is worth reiterating the need for the PIPPs to include the requirement that notice of the circumstances of the data collection must be provided prior collection, as well as disclosure who else may have access to that data once collected. These points are key to the provision of informed consent.

Similarly, the expansion of the current requirement that the collection is lawful, to also have to be 'fair', as is currently required by the APPs, is strongly supported.

Question 2.9

Should any of the other potential reforms be introduced, including:

a. fairness and reasonableness requirements;

b. a right to object;

c. a right to be forgotten;

d. specific restrictions on the use of artificial intelligence in automated administrative decision-making; or

e. strengthened notice and consent requirements?

Yes to all of the above. Further, consideration should also be given to the additional requirement collecting authorities should indicate the duration that it is intended for that personal information to remain stored, accessible and used. For example, the COVID-related Check-in TAS App data was to be deleted after 28 days. There may be functions or reasons for personal information collection to occur where it is anticipated it will only be used or pertinent for a set and specified period of time. There should be a requirement that individuals are informed whether the intent is for indefinite storage, and if not the expected timeframe by which that data will eb partially or wholly deleted, and to also receive confirmation once that erasure has occurred.

Chapter 2—Privacy protection: Complaints, monitoring and enforcement

Question 2.10

How effective is the current complaints process in enforcing obligations under the PIPA?

It is difficult to answer this specific query in light of the restricted nature of the available data. On one hand the current capacity of the Tasmanian Ombudsman to act upon received complaints appears sound and rigorous – in that the Ombudsman can make any recommendations considered necessary which must be tabled in both Houses of Parliament within 5 sitting days of receipt.

However, the current data does not detail whether those recommendations were acted upon, or how effectively they were implemented, or any long-term educative influence those determinations may have had on the culture of the particular public information custodian involved.

Statistics detailing the number of complaints dealt with by the Ombudsman does not provide qualitative assessment of the effectiveness of complaint assessment processes.

Further, the capacity for the Ombudsman to initiate own motion investigations would add rigour to PIPA compliance in general.

Question 2.11

Should consideration be given to amending the PIPA to include provision for an individual to appeal or seek review if they are dissatisfied with the actions or recommendations of the Ombudsman in investigations of privacy complaints?

Yes. This is available in NSW, Victoria and federally. Informed consent is also informed by an understanding of, and confidence in, available mechanisms of appeal and/or redress where appropriate.

Question 2.12

What other remedies should be available to individuals affected by a breach of the PIPA?

As per privacy legislation in Queensland, NSW and Victoria, amending the PIPA to provide for compensation for a breach of privacy principles should be considered.

Question 2.13

Are there other forms of enforcement action that should be introduced?

Inclusion of a range of civil penalty measures such as provided for under the federal Privacy Act should be investigated.

Question 2.14

Should consideration be given to the development of privacy codes by amendment to the PIPA or by providing for similar rules to be made in delegated legislation?

Yes. The PIPA should provide mechanisms for the development, consultation, approval and review of binding privacy codes. Specifically, any such privacy code needs to have the legislated status that a breach of the code has the same legal effect as a breach of the privacy principles as a minimum.

Question 2.15

Should a form of data breach notification requirement be introduced? If so, what models of mandatory reporting schemes should be considered?

Yes. Recent data breaches, such as that experienced by the Tasmanian Education department, have highlighted the public expectation that affected individuals would be informed in a timely manner by authorities.

Further, it should be a legislated requirement that should there be reasonable grounds to suspect there has ben a data breach, the authority or entity must investigate to ascertain whether there are reasonable ground to consider the breach did occur.

Chapter 3— Other legislation impacting the privacy of government held information

Question 3.1

Should legislation providing for the application of minimum privacy safeguards be introduced to apply to all information sharing within and between government bodies?

Yes. And it must apply to all tiers of government bodies (ie local government and federal government), including contractors and sub-contractors.

Question 3.2

If such legislation should be introduced, how should the safeguards be enforced?

Potentially via stipulated regular independent auditing by all tiers of government involved, (ie the OAIC should the Commonwealth be an involved jurisdiction plus the State Ombudsman) to allow for cross-referencing checks, with those reports to be tabled in respective Parliaments.

Further appeal to courts and/or compensation measures may also be applicable.

Chapter 4— Other protections of privacy

Question 4.1

Should the existing protections in the listening devices legislation be amended in Tasmania to strengthen the protection of individuals against surveillance, whether governmental, workplace, or private surveillance?

Yes.

Question 4.2

Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against governmental (particularly police) surveillance in general?

Yes. Including greater independent transparency, assessment, and reporting mechanisms, and appeal rights.

Question 4.3

Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against workplace surveillance in particular?

Yes.

Question 4.4

Should there be specific protection against interference with physical privacy through the use of drones (Remotely Piloted Aircraft or RPAs, and Unmanned Aerial Vehicles or UAVs)?

Yes. These forms of technology can be applied in an indiscriminatory manner which can have serious implications for minors and other vulnerable members of the community.

Question 4.5

Are the existing legislative protections against stalking and harassment adequate to protect physical privacy, or should there be a new or strengthened law to protect against such physical and intimidating interferences?

This submission acknowledges concerns raised about current inadequate protections but does not present an opinion on how to best remedy the situation.

Question 4.6

Are the existing legislative protections (largely at the Commonwealth level) against image-based abuse and similar online privacy interferences adequate to protect individual privacy, or should the Tasmanian Parliament enact new criminal offences or civil remedies for such egregious online interferences with privacy, as other Australian jurisdictions have done?

The Tasmanian Parliament should enact new criminal offences, or at least civil remedies, for against image-based abuse and similar online privacy interferences, consistent with other Australian jurisdictions.

Question 4.7

Does existing judicial recognition of privacy (either through equitable remedies or as a nascent constitutional principle) provide adequate protection for individual privacy, especially in circumstances not covered by the PIPA and other legislative protections?

No, not necessarily.

Question 4.8

Should Tasmania codify a fundamental right to privacy, which can be set aside by other legislation that authorises activities that may interfere with privacy, and which is qualified by justified limitations?

Yes. As stated above, the TLRI recommended Human Rights Charter included the right to privacy back in 2007. A comprehensive Tasmanian Human Rights Act, or Charter, should be legislated to provide a coherent and comprehensive framework in which our privacy statues are derived and embedded.

Conclusion

This independent review of Tasmania's Privacy Laws is timely.

Events occurring over recent years, including the COVID-19 pandemic and examples of governments and the private sector selectively utilizing technological developments to 'harvest' individuals' sensitive and personal information in an ad hoc and potentially unregulated manner demonstrate the inadequacy and fragmentation of existing legislation.

This legislative fragmentation combined with varying degrees of understanding of the human right to privacy, rights and responsibility regarding accessing, using, transferring, storing, deleting sensitive and personal data, and continuing technological developments provides current and future potential for real and damaging abuse and human rights infringements.

Many of the responses to the above consultation questions are provided as in-principle positions, noting that some would be subject to adequate funding, resourcing and enforcement considerations and measures.

It is also worth reiterating that a crucial first step is the implementation of a legislated Tasmanian Human Rights Charter in which the state's privacy laws should be embedded.

Further, in recognition of the federal government's review of the Commonwealth *Privacy Act 1988* there should also be consideration of potential future model legislation being developed, either as once comprehensive legislative framework, or focused on more specialized specific areas such as facial recognition technology as attempted with the now-stalled *Identity-matching Services Bill 2019.* While the state and its citizens cannot afford to wait indefinitely for national agreement on model legislation with the primary focus of protecting privacy rights, it does add impetus for Tasmania to ensure its current laws set a high standard.

Lastly, any proposed reforms to Tasmania's *Personal Information Protection Act 2004* must also be accompanied with specified enforcement and resourcing recommendations. Similarly, a focused and resourced public education campaign that is driven by an understanding of the right to privacy at its core, consistent with our obligations under the *International Covenant on Civil and Political Rights* is required.

References:

Australian Privacy Foundation, August 2018, *Privacy in Australia: Brief to UN Special Rapporteur on Right to Privacy,* Australian Privacy Foundation, Australia.

Government Response to the Privacy Act Review Report (Cth), 16 February 2023, Commonwealth of Australia.

Parliamentary Joint Committee on Human Rights, June 2018, *Report 5 of 2018,* Parliament of the Commonwealth of Australia.

Parliamentary Joint Committee on Intelligence and Security, October 2019, *Advisory report on the Identity matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*, Parliament of the Commonwealth of Australia.

Personal Information Protection Act 2004 (Tas)

Tasmania Law Reform Institute, March 2023, *Review of Privacy Laws in Tasmania*, (Issues Paper No 32), University of Tasmania.

Tasmania Law Reform Institute, October 2007, *A Charter of Rights for Tasmania*, (Report No. 10), University of Tasmania.

Tasmania Law Reform Institute, October 2007, *Charter of Rights Recommended for Tasmania*, Media Release, University of Tasmania.

Tasmanian Liquor and Gaming Commission, June 2022, *Investigation of harm minimisation technologies: facial recognition and player card gaming Report to the Treasurer*, Department of Treasury and Finance.

Appendix A: Tasmanian Parliamentary Questions re the National Driver Licence Facial Recognition Solution

Questions asked by the Hon. Meg Webb MLC on 5 June 2023 and answered by the Hon. Michael Ferguson MP, Minister for Infrastructure and Transport, on 15 June 2023 (delivered in Parliament on Tuesday 27 June 2023).

With regard to the Minister's response dated the 1st of June on the matter of the National Driver Licence Facial Recognition Solution (the "Solution') and the Tasmanian data supplied by the state government to the Solution, can the Government clarify the apparent discrepancy between answers 1 (b) and 2 (b), specifically:

1. How does the Minister's response to 1(b) that, "*post 20 October 2020, 25,648 records have been provided, comprising new and updated records*" to the Solution, reconcile with the subsequent response to 2(b) which states the daily upload of records to the Solution "*has been paused since 20 October 2020*" ?;
2. Detail the manner by which 25, 648 new and updated records were provided to the Solution since 20 October 2020, if they were not provided via an upload of daily files?; and
3. Clarify whether the 25, 648 new and updated records provided since 20 October 2020 were in fact drivers licence records or any other form of Tasmanian records?

ANSWER:

1. Unfortunately, the advice previously provided based on information from the Department of State Growth was incorrect. The number of records provided post 20 October 2020 is 25,648. The daily transfer has been paused since 16 December 2020.
2. The 25,648 records were uploaded to the Solution through contemporary web services security standards with strong encryption protocols and hardened ciphers. Additionally, the exchange is digitally signed, so that they cannot be tampered with without detection.
3. The 25,648 records provided were driver licence records. Tasmania has not uploaded into the Solution any records other than driver licences. There are no current plans to load any other government issued identification records into the Solution. This would only be done through legislative changes.

Questions asked by the Hon. Meg Webb MLC on 25 May 2023 and answered by the Hon. Michael Ferguson MP, Minister for Infrastructure and Transport, on 1 June 2023

With regard to the National Driver Licence Facial Recognition Solution (the "Solution') and the Tasmanian data supplied by the state government to the solution, can the Government:

1. Detail the total number of Tasmanian drivers' licence images provided to the Solution for the periods:
   (a) up to 20 October 2020; and
   (b) since 20 October 2020?
2. Advise whether Tasmania's segment of the Solution where Tasmanian drivers' licence images are stored, continues to be maintained, and if so, further detail;
   (a) who is responsible for that maintenance; and
   (b) what is involved in maintaining Tasmanians' data on the Solution?
3. Advise whether access has been granted to the Tasmanian segment of the Solution to any entity other than the Tasmanian Department of State Growth, and if so detail to whom and for what purpose?
4. Advise whether:
   (a) Commonwealth Legislation has been introduced to Federal Parliament or passed by Federal Parliament to govern use of images provided to the Solution; and

(b) the state government has liaised with its federal counterparts over the content of any such federal legislation?

ANSWER:

1(a). As of 20 October 2020, 442,744 driver licence records were provided.

1(b). Post 20 October 2020, 25,648 records have been provided, comprising new and updated records.

2(a). The provision of new and updated Tasmanian driver licence data continues to be on hold due to system upgrades not being finalised by the Commonwealth Department of Home Affairs. That department is responsible for maintenance of the Solution software.

2(b). All Tasmanian driver licence records continue to be managed by the Department of State Growth. The department does not currently maintain any records directly within the Solution. Records are maintained through an upload of daily files to the Solution; however this has been paused since 20 October 2020.

3. No access has been provided for the use of or validation of Tasmanian driver licence images.

4(a). At present there is no current tabled or passed Commonwealth legislation to govern the use of images provided to the Solution.

4(b). The Department of State Growth has previously liaised with Department of Home Affairs over the content of the proposed legislation. However, it is unclear what approach the Australian Government intends to take next

Questions asked by the Hon Meg Webb MLC on 28 July 2021. Answered by the Hon Michael Ferguson Minister for Infrastructure and Transport on 24 August 2021.

QUESTION

(1): In October 2020 in response to the Legislative Council e-Petition No. 33 Transfer of driver licence photos to National Driver Licence Facial Recognition Solution, and in relation to the Commonwealth legislation to support implementation of Face Matching Services, the Premier said that:

Until this has been passed and I receive advice that Tasmanian legislation fully supports the use for the purpose reflected in this bill, Tasmanian data that is currently in a segregated partition of the National Driver Licence Facial Recognition system will not be available for use by any other agency or jurisdiction.

Is the Premier's statement supported by any written assurance from those responsible for the National Driver Licence Facial Recognition system (NDLFRS) to the Tasmanian Government or elsewhere that Tasmanian data in the segregated partition will not be available for use by another agency or jurisdiction?

a) If yes, please provide a copy of that assurance. **b)** If no, what is the basis for the Premier's assurance?

QUESTION (2): The Premier also said that he understood, I quote:

The Australian Government is proposing to introduce legislation later this year, i.e, 2020, to support implementation of Face Matching Services.

Is Tasmania continuing to provide Tasmanian drivers licence data to the NDLFRS despite the fact that no Commonwealth legislation has been passed?

QUESTION (3): Has any Tasmanian drivers licence data been used in the 'limited (low volume) trial' of the Face Matching Service (FMS) by the New South Wales Police Force?

QUESTION (4): Has any Tasmanian drivers licence data in the segregated partition of the NDLFRS been made available for use by another agency or jurisdiction since the Premier's assurance?

ANSWER (1) Commonwealth legislation has not yet been passed to enable the National Driver Licence Facial Recogition System. Tasmania has not, and will not, enter into a Participant Access Arrangement with any agency for access to Tasmanian data until Commonwealth legislation has passed.

ANSWER (2) The provision of Tasmanian driver licence data has been temporarily paused due to system upgrades initiated by the Department of Home Affairs. I am advised that this system upgrade is planned to be finalised by the end of September 2021. The delay in the passing of Commonwealth legislation is deferring Tasmania's access to improve identity protection from the rollout of the FMS.

ANSWER (3) There has been no access provided to Tasmanian driver licence data. In relation to the use of FMS, the New South Wales Police article referenced in this question confirms 'specialist New South Wales PF officers have limited access to the FMS using facial images from Commonwealth agencies'. For example, photographs of passport and visa holders issued by the Department of Foreign Affairs and Trade.

ANSWER (4) The Tasmanian driver's licence data in the segregated partition of the NDLFRS has not been made available to any other agency or jurisdiction.

Questions asked by the Hon Meg Webb MLC on 15 October 2020. Answered by the Hon Michael Ferguson Minister for Infrastructure and Transport on 11 Nov 2020.

With regard to the National Driver Licence Facial Recognition Solution (NDLFRS):

Question 1. Can the Government provide details on—

(a) the total number of Tasmanian drivers' licences images and associated data provided to the NDLFRS; and

(b) the timeframe during which that Tasmanian information was and/or continues to be provided to the NDLFRS system?

Answer (1)(a) All Tasmanian driver licences are replicated in the secure Tasmanian segment of the NDLFRS. As at 20 October 2020, there are 442 744 Tasmanian driver licences, accessible only by the Tasmanian Department of State Growth.

Answer (1)(b) Tasmania's segment of the NDLFRS was initially loaded with data in December 2018 and continues to be maintained.

Question 2(a) Given the absence of the necessary national legislation, are Tasmanian drivers' licences images and associated data currently still being provided to the NDLFRS system;

(b) if not, please advise the date it ceased; and

(c) if so, why is that the case?

Answer (2)(a) The data continues to be replicated to a segment of the NDLFRS managed by and only accessible to the Tasmanian Department of State Growth. No further access has been granted to this data.

Answer (2)(b) N/A

Answer (2)(c) Once fully implemented, with all appropriate legislative protections and provisions, Tasmanians will be at the forefront in protection from identity fraud, a crime costing the nation in excess of $3.1 billion annually. Tasmanians will directly benefit from this initiative when operational.

Question (3) With regard to the following classes of Tasmanian drivers' licences images and associated data to the NDLFRS can the Government provide (a) the details on data provided and (b) the number for each class:

(a) renewal of full drivers licences;

(b) new drivers licences,

(c) new provisional drivers licences; and

(d) current drivers licences granted prior to 2017?

Answer (3) The data that is stored and only available to the Department of State Growth, for all licence holders, is: Surname, Other Names, Date of Birth, Licence Number, Expiry Status and Image, noting the class of licence is not replicated.

Answer (3)(a) There have been 377 140 driver licence renewals from 1 January 2017 to 20 October 2020.

Answer (3)(b) 29 276 full driver licences were issued in the period 1 January 2017 to 20 October 2020 including clients who have moved from Provisional to Full licence holders.

Answer (3)(c) There were 25 829 Provisional driver licences issued from 1 January 2017 to 20 October 2020, noting a number of these holders are now Full licence holders.

Answer (3)(d) As at 20 October 2020, 348 857 Tasmanians with an active driver licence obtained their licence in Tasmania prior to 1 January 2017.

Question (4) Can the Government detail the privacy, legislative and other provisions applied to the collation and supply to the national database of Tasmanians drivers' licence images and associated data?

Answer (4) Each aspect of the Face Matching Services program has been subject to an Independent Privacy Impact The power to store the data exists under the *Vehicle and Traffic Act 1999* for the initial purpose of maintaining integrity of driver licences.

Question (5) (a) Given the absence of the necessary national legislation for the operation of the NDLFRS, will the Government recall Tasmanians' data already provided; and

(b) if not, why not?

Answer (5)(a) The absence of the national legislation is a matter for Federal Parliament to determine and only after that has occurred would Tasmania participate in the national system.

Answer (5)(b) The work completed will ensure Tasmanians will be at the forefront of digital identity management and will receive the personal protection benefits this will provide, specifically, protection from identity fraud. Facial recognition is used widely to protect key photo identity documents utilised in the Australian community, including Passports and Visas, and currently by three other driver licensing jurisdictions which have run their own facial recognition programs for a number of years.

Question (6) In response to Legislative Council Petition No. 33 of 2020 the Government has stated that "Tasmanian legislation fully supports the use for the purpose reflected in this bill". Will any eventual national legislation be tabled in the Tasmanian parliament?

Answer (6) It is not intended to table the Commonwealth Legislation as application legislation in Tasmania.

Question (7) (a) Can the Government guarantee there will be a moratorium on any use of Tasmanian drivers' licence images and any associated data currently transferred to the NDLFRS, until such transfer is authorised under an Act of the Tasmanian Parliament; and

(b) if not, why not?

Answer (7)(a) On passing of the Commonwealth Legislation, Tasmanian Legislation will be reviewed to confirm that it complements and supports this legislation. Until such time, the Tasmanian data is not accessible by any other government or authority and remains secure in a separate segment.

Answer (7)(b) Use of the data will not occur until the Commonwealth Legislation has passed and Tasmanian Legislation is reviewed.

Question (8) (a) Can the Government guarantee there will be a moratorium on any future transfer and use of new Tasmanian drivers' licence images and any associated data, until such transfer is authorised under an Act of the Tasmanian Parliament; and

(b) if not, why not?

Answer (8)(a) The Tasmanian Legislation will be reviewed in context of the Commonwealth Legislation. There will be no access provided to the data to any party other than the Department of State Growth until this occurs.

Answer (8)(b) The Department of State Growth will continue to maintain records that are stored within the secure Tasmanian segment of the NDLFRS. This will ensure Tasmanians to obtain the benefits of improved identity protection as soon as Face Matching Services is extended to enable validation of driver licences.

Questions by Meg Webb MLC on 28 Nov 2019 answered for the Govt by Michael Ferguson MP, Minister for Infrastructure & Transport on 17 Mar 2020

Question 1. What legislative authority does the Register rely upon for secondary collection of facial data for the purposes of the 2017 Intergovernmental Agreement on Identity Matching Services not relating to the functions of the Registrar under section 6 of the Vehicle and Traffic Act?

Question 2. In the notice of the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Amendment (Identity Matching Services) Regulations 2017*, it was stated that the regulations would :

"amend the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* to allow the Registrar of Motor Vehicles to divulge information in accordance with the Intergovernmental Agreement on Identity Matching Services"

a) Noting the regulations may only be issued within the jurisdiction of the Act (common law/section 45 VTA) what legislative authority does the Registrar rely upon for the issuing of regulations for each and every purpose set out in clause 1.2 of the Intergovernmental Agreement on Identity Matching Services?

b) If the above stated regulations related only to the divulging of information, under what authority has the Registrar been collecting facial records for purpose of the Intergovernmental Agreement on Identity Matching Services?

ANSWER Questions 1 & 2: Driver licences are the most common form of identification used in Australia and are, therefore, a target used by criminals, including organised crime, to assume someone's identity or create a false one. New identities are also created to obtain a new driver licence to avoid licence suspension. The new service will be a tool to assist the Registrar of Motor Vehicles (Registrar) and Tasmania Police to detect duplicate and false identities, thereby maintaining the integrity of driver licences and limiting opportunities for identity fraud and other identity-based crime.

The collection of facial images for driver licences has been in place for nearly 30 years. The *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (the Licensing Regulations), in particular regulations 20, 25, 29 and 138, is the current legislated authority for the collection of these images. The requirement to divulge images for the purposes of Identity Matching Services has not resulted in the collection of any additional information or images. The Registrar already held this information for the purposes of driver licensing.

In regards to the questions you have raised the following information is provided.

The data provided in accordance with the 2017 Intergovernmental Agreement on Identity Matching Services (the Agreement) is already held in the registers maintained by the Registrar. No additional data is collected for the purposes of the Agreement. These registers, and the Registrar's powers to release information from them, have been created under the authority of s41 of the *Vehicle and Traffic Act 1999* (the Act).

The data transferred into the segregated National Driver Licence Facial Recognition Solution (NDLFRS) database is a subset of the register of driver licences. The driver licence register is required to be kept under regulation 124 of the Licensing Regulations.

The Registrar maintains and owns the data in NDLFRS, and no other jurisdiction or agency is able to amend or delete or add data into this segregated database. The National Exchange of Vehicle and Driver Information System (NEVDIS) also contains a subset of the driver licence register except for images and has done so for a number of years.

Question 3. Under clause 2 of the Intergovernmental Agreement, Tasmania agreed that:

"the design and operation of the Identity Matching Services adopt robust privacy safeguards, informed by independently conducted privacy impact assessments, developed in consultation with federal and state privacy commissioners (or equivalents), to balance privacy impacts against the broader benefits to the community from sharing and matching identity information"

a) What specific privacy assessment was undertaken in respect of this undertaking prior to the collection of data of the Face Verification Service?

b) When was this privacy assessment undertaken?

c) On what basis was an exemption for the completion of a regulatory impact statement granted that means no RIS was conducted on the amendments to the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010*?

d) How does the secondary collection of data to the Face Verification Service database comply with Privacy Information Principle 1, under Schedule 1 of the *Personal Information Protection Act*?

ANSWER: The Registrar is empowered to divulge protected information from the driver licence register in accordance with regulation 125 of the Licensing Regulations.

Additionally, divulging information for the purposes of Identity Matching Services under the Agreement is also consistent with Personal Information Protection Principles set out in the *Personal Information Protection Act 2004* (PIP Act). These Principles allow for the disclosure of personal information for a purpose other than the purpose for which it was collected if the disclosure is reasonably necessary for law enforcement purposes.

A comprehensive set of safeguards were developed in consultation with federal and state privacy commissioners including the Tasmanian Ombudsman.

Question 4. The Legislative Council was informed at the briefing on 28 November 2019 that a regulatory impact statement was not prepared for the Subordinate Legislation Committee under section 5 of the *Subordinate Legislation Act*?

a) Were the burdens on community and individual privacy considered in determining not to issue a regulatory impact statement?

b) Did the Registrar or Department explicitly advise the Minister no part of the regulations would impose any significant burden, cost of disadvantage on any sector of the public?

c) Did the Registrar or Department make an assessment as to whether or not the regulation was "within the regulation-making power conferred by, or in accord with the general objects of, the Act pursuant to which it is made"?

ANSWER: In accordance with the *Subordinate Legislation Act 1992*, an assessment of this amendment was undertaken and received endorsement from the Department of Treasury and Finance in November 2017 and final determination was given in December 2017 that a Regulatory Impact Statement was not required as the regulation did not impose a significant burden, cost or disadvantage on any sector of the public.

The then Minister for Infrastructure provided a certificate of compliance that the guidelines were followed in accordance s4 of the *Subordinate Legislation Act 1992.*

This was provided to the Subordinate Legislation Committee in January 2018.

Questions by Hon Meg Webb MLC on 4 Nov 2019 answered for the Govt by Hon Will Hodgman Premier on 21 Nov 2019

In response to the Government's answer to the question put by the member for McIntyre on 31 October 2019 in relation to consent to the collection and storage of biometric data of Tasmanians for use in the National Driver Licence Facial Recognition Solution –

Question (1) What assessment was undertaken to ensure the collection of data for this purpose is compliant with the Personal Information Protection Act 2004?

ANSWER (1) The Registrar of Motor Vehicles – the registrar – was satisfied there was legislative authority for the disclosure of driver licence images for identity-matching purposes. However, to give additional certainty, the relevant provisions of the Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010 were amended to specifically cover disclosure for this purpose.

The Personal Information Protection Act 2004 – PIP act – allows for the disclosure of personal information for the purpose for which it was collected, which includes national identity-matching services as noted in the personal information collection statement.

The PIP act also allows for disclosure for a purpose other than the purpose for which it was collected if that disclosure is reasonably necessary for law enforcement purposes, including the prevention and detection of identity crime.

Question (2) How is the collection and storage of biometric data for the purposes set out in the Intergovernmental Agreement on Identity Matching Services made between the Tasmanian Government and the Commonwealth, states and territories in October 2017 compliant with the Personal Information Protection Act 2004, in particular Schedule 1, clauses 1, 2, 5 and 6, noting that intergovernmental agreement-specified data is to be used not for vehicle licensing and driver identification but for preventing identity crime, general law enforcement, national security, protective security and community safety?

ANSWER (2) Clause 1 of Schedule 1 of the PIP act deals with the collection of personal information. The collection of photographs and other identifying information is a statutory requirement for the issuing and renewal of driver licences. There is no additional information collected for the purposes of identity-matching services.

Clause 2 of Schedule 1 allows for disclosure of personal information other than for the purpose for which it was collected if that disclosure is reasonably necessary for law enforcement purposes. On this basis, the provisions of the PIP act are not inconsistent with the specific provisions in the licensing regulations that permit disclosure for the purposes of identity-matching services and the two provisions can operate concurrently.

Clause 5 of Schedule 1 of the PIP act deals with documentation of policies for the management of personal information. The disclosure of personal information for the purpose of identity-matching services is clearly set out in the intergovernmental agreement. This agreement may be provided on request to anyone who asks for it, in accordance with section 5 of Schedule 1 of the PIP act. This information is also available via the Department of State Growth's Transport website at www.transport.tas.gov.au

In accordance with clause 6 of Schedule 1 of the PIP act, individuals may access their personal information held in the driver licence register by submitting a request to the registrar. Information regarding this process is available on the Transport website.

Question (3) Why did the Government not refer the terms of the agreement to a parliamentary committee or seek amendment of primary legislation through the parliament to support Tasmania's participation in the national identity-matching services regime?

ANSWER (3) The changes made to the regulations followed the national agreement at COAG in October 2017 for the establishment of national identity-matching services. The amended regulations were published in late December 2017, tabled in both Houses of parliament in June 2018 and examined by the Subordinate Legislation Committee later the same month. The Government has provided full public and parliamentary review of these changes, the legal provisions used and the reasons for doing so.