Office of the Information Commissioner
Queensland

20 April 2020

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

Committee Secretary
Transport and Public Works Committee
Parliament House
George Street
Brisbane Qld 4000

By email: tpwc@parliament.qld.gov.au

Dear Ms Jeffrey

Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Bill 2020

The Queensland Office of the Information Commissioner (**OIC**) appreciates the opportunity to provide a submission to the Transport and Public Works Committee (**the Committee**) on the Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Bill 2020 (**the Bill**).

Information Privacy Act 2009

Queensland's *Information Privacy Act 2009* (**IP Act**) recognises the importance of protecting the personal information of individuals. It creates a right for individuals to access and amend their own personal information and provides rules or 'privacy principles' that govern how Queensland government agencies collect, store, use and disclose personal information. OIC has regulatory oversight of Queensland Government agencies' compliance with requirements under the IP Act.

As outlined in the Explanatory Notes, the Bill the objectives of the Bill are:

- to support the introduction and ongoing operation of a Digital Licence App
- facilitate camera enforcement of seatbelt and mobile phone offences; and
- make minor and technical improvements to various provisions in several Acts.

Both the Camera Detected Offence Program (**CDOP**) and Digital Licence APP (**Digital Licence APP**) raise privacy issues. While the right to privacy is not absolute, an appropriate balance must be struck between privacy and other legitimate rights and interests. Failure to put in place adequate measures to protect an individuals' personal information erodes trust, jeopardises public take up of services, damages an agency's reputation and exposes these individuals to risk.

The Department of Transport and Main Roads (**TMR**) consulted OIC on the proposed introduction of a CDOP and Digital Licence APP at varying points throughout the development of both these initiatives. OIC reviewed and commented on a preliminary draft of the Privacy Impact Assessment (**PIA**) for the CDOP. However, OIC was not consulted on the draft Bill which provides the legislative framework to support introduction of the CDOP and Digital Licence APP. OIC's comments on the

provisions of the Bill regarding the CDOP and Digital Licence are dealt with separately below:

1. CDOP

Privacy concerns are inherent in a program that relies on high definition photographic images taken inside an individual's motor vehicle. The CDOP Project involves the majority of the IPPs in the IP Act, fundamentally starting with collection through to storage and security, access, use and disclosure.

As noted earlier, while the right to privacy can be limited, any interference must be reasonable, necessary and proportionate to achieving a legitimate policy goal. As such, an appropriate balance must be struck between the legitimate policy goal of improving road safety and reducing road trauma and incursion into an individuals' privacy.

a) Privacy and Security measures

The Explanatory Notes to the Bill outline a number of privacy and security measures to mitigate risks arising from the use and storage of information captured by the cameras including:[1]

- encryption of image files for detected offences and transferring data via secure networks
- contractually binding the camera supplier to the *Information Privacy Act 2009* (**IP Act**)
- subjecting supplier personnel that have access to images to a criminal history check and training
- access logs to the images to determine who has accessed what image; and
- ensuring controls over physical access to the camera sites.

The Explanatory Notes also state that it is proposed to release a PIA for the CDOP, once completed, and notes information about the camera system and how data will be managed will be made publicly available.[2] While OIC supports these measures to mitigate the privacy and security risks of the CDOP, OIC may wish to further comment on these measures, including any additional measures that may be required, once the PIA is released. OIC also recommends updating the PIA throughout the lifecycle of the CDOP.

b) Proposed legislative amendments

OIC notes that the Bill provides for some matters regarding operation of the CDOP to be prescribed by regulation. These matters include:

- procedures for verification of offences (new section 113A(4)(a)). For example, requirement for human oversight by Queensland Police Service (**QPS**) of potential offences detected by the machine learning algorithms before any infringement notice is issued; and

[1] at page 12.
[2] at page 12.

- deletion of data where there is no offence detected by the device or system (new section 113A(4)(b)).

OIC further notes that the meaning of '*prescribed offences'* in the *Transport Operations (Road Use Management) Act 1995* (**TORUM Act**) is prescribed by regulation. While OIC notes it is intended that camera-detected enforcement of mobile phone and seatbelt offences will be managed within the existing legislative framework for camera-detected offences (outlined in Chapter 5, Part 7 of the **TORUM Act)**, OIC considers the types of offences for which this more invasive technology can be used is not sufficiently limited by the proposed amendments contained in the Bill.

Further, the use of artificial intelligence to determine whether an offence has occurred requires safeguards to ensure there is transparency around the use of this technology. The use of artificial intelligence also raises potential human rights considerations. OIC agrees with the finding of the NSW legislative Council, following its examination of legislative amendments to facilitate the introduction of the NSW Digital Licence, 'that there should be transparency in how the artificial intelligence identifies potential offenders including the ability to test whether or not the algorithms contain any inadvertent or inherent biases'.[3]

As noted previously, the digital video technology used for detecting mobile phone use and seat belt offences allows high definition photographs images to be taken inside an individual's vehicle. This contrasts with the less privacy invasive nature of images captured under the existing camera detected offences such as speeding and disobeying red traffic lights, which typically captures the exterior of a vehicle including vehicle registration numbers.

While OIC notes the Bill provides that procedures for verification of offences will be prescribed by regulation, regulations are not subject to the same level of parliamentary oversight and scrutiny as primary legislation. To strengthen privacy protections, OIC recommends inclusion of the following express legislative provisions in the Bill to:

- clearly define and limit the offences when using this more invasive technology to mobile phone use and seatbelt infringements to prevent scope creep
- require human oversight in the determination of whether an offence has occurred
- prohibit transfer of data to QPS that do not contain evidence of an offence
- impose an obligation to permanently delete photographs that do not give rise to the issuing of an infringement notice for the above offences, and;
- specify a timeframe for the deletion of images which do not depict an offence. This timeframe should be the shortest possible time the technology requires to achieve this outcome. As outlined in the Explanatory Notes, a key element in upholding and protecting a person's right to privacy will be that images or video that do not contain evidence of an offence will be deleted by the system and are not used or transferred to a human.

[3] NSW Legislative Council, Road Transport Amendment (Mobile Phone Detection) Bill 2019 Report No 52 – November 2019 at page 26.

Should the above matters continue to be dealt with by regulation, OIC would welcome further consultation on the development of these regulations. Given the regulations are yet to be drafted, OIC is unable to fully consider the privacy implications of the Bill. As such, OIC may wish to make further comment once the regulations, if any, are drafted.

2. Digital Licence APP

As outlined in the Explanatory Notes,[4] the Digital Licence APP is likely to provide additional benefits for Queenslanders including providing customers with greater security, protection and control in sharing their information by leveraging data encryption and phone security to protect customers. OIC considers the Digital Licence App can enhance privacy protections for individuals by allowing individuals to control the amount of personal information released to others.

OIC was consulted by TMR on the privacy enhancing features of the technology used in the development of the Digital Licence App and welcomes these initiatives, in particular, compliance with international standard ISO 18013-5.

a) Public release of the PIA

The Explanatory Notes state that an independent PIA was undertaken in relation to the Digital Licence APP.[5] In the interests of transparency and accountability, OIC recommends the PIA be made publicly available. Community concerns over privacy and the government's ability to protect their personal information and secondary use of data, whether real or perceived risks, have the potential to undermine community trust and confidence resulting in reduced levels of take up by the community.

Release of the PIA publicly, in conjunction with a comprehensive community education program about the operation of the Digital Licence App is essential in building community trust and confidence in new programs and initiatives such as the Digital Licence App. OIC also recommends updating the PIA throughout the lifecycle of the Digital Licence App.

b) Production of digital drivers' licence

OIC previously raised concerns with TMR about the need to include an express legislative provision prohibiting QPS or an authorised officer from requiring an individual to hand over their electronic device when requested to produce their digital driver licence.

OIC notes that the Bill makes amendments to several Acts to limit the seizure and confiscation powers of an 'authorised officer' or 'inspector' for evidentiary purposes.[6] OIC further notes that new sections 29AH and 29AI of the *Transport*

[4] at page 2.
[5] at page 16.
[6] For example: Amendment of *Gaming Machine Act 1991* (Clause 4 inserts subsection 257(3)). Section 257(3) clarifies the seizure and confiscation powers and obligations in section 257 (Seizure of document wrongly used as evidence of age); *Amendment of Keno Act 1996* Clause 11 amends section 184 by inserting subsections (2) and (3). Section 184(2) and the related definitions in (3) clarify the seizure and confiscation powers and obligations in section 184 (Seizing evidence at keno gaming places; Amendment of *Liquor Act 1992 Clause 15 inserts*

Planning and Coordination Act 1994 ensure that requirements to produce, give or make available for inspection, a drivers licence or evidence of age of identity, can be satisfied by the display of a digital authority, digital evidence of age or digital evidence of identity through an approved app.

However, these amendments do not make it clear that a person is not required to hand over to the person, who is requiring the driver licence to be produced, the mobile phone or other electronic device on which the digital driver licence is displayed. The interaction with various provisions of the *Police Powers and Responsibilities Act 2000* is also unclear.

A mobile device contains a large amount of personal information of both the user and other persons. Requiring an individual to hand over a mobile device for the purposes of displaying a digital driver licence represents a significant incursion into the privacy of the individual and potentially other individuals. Any limitations on an individual's right to privacy must be reasonable and necessary to achieve the stated purposes and subject to appropriate and ongoing accountability measures, including independent review about how the powers are used.

To ensure clarity and certainty around requirements regarding production of a digital driver licence, including use of a digital driver licence to satisfy evidence of identity, OIC recommends inclusion of an express provision in the Bill that aligns with the recent amendment to the NSW *Road Transport Act 2013* to facilitate introduction of a digital driver licence. Section 61C(4) is extracted below:

> (4) Despite any other provision of this section, a person who displays or purports to display a digital driver licence is not required to give or hand over, to the person who is requiring the driver licence to be produced or handed over, the mobile phone or other electronic device on which the digital driver licence is displayed or purported to be displayed.

OIC notes that during the second reading speech for the NSW Road Transport and Other Legislation Amendment (Digital Driver Licences and Photo Cards) Bill 2018, the Hon. Catherine Cusack stated:

> '*a mobile device is so much more than just a digital driver licence. A phone is a person's personal property and may also be used to store and access personal and private information. To ensure appropriate privacy and a citizen's right to maintain control of their personal electronic device, a driver will only need to display their digital driver licence on their device to the police or authorised officer in order for their digital driver licence to be checked.*
>
> *I am pleased that the Privacy Commissioner has supported this approach, stating, "This will ensure the privacy rights of an individual who holds personal information on their phone beyond the digital driver licence is preserved*'.[7]

---

subsection 160(3). Section 160(3) clarifies the seizure and confiscation powers and obligations in section 160 (Seizure of document wrongly used as evidence of age); Amendment of TORUM Act Clause 48 inserts subsection 40(5). Section 40(5) clarifies the seizure powers and obligations in section 40 (Power to seize evidence).

[7] https://www.parliament.nsw.gov.au/Hansard/Pages/HansardResult.aspx#/docid/'HANSARD-1820781676-76486' Second Reading Speech, The Hon. CATHERINE CUSACK, 23 May 2018

OIC remains available to assist the Committee.

Yours sincerely

Philip Green
Privacy Commissioner

Rachael Rangihaeata
Information Commissioner