Transport (New Queensland Driver Licensing) Amendment Bill 2008

Explanatory Notes

General Outline

The Bill amends the following five Acts—

- *Police Powers and Responsibilities Act 2000;*
- *Tow Truck Act 1973;*
- *Transport Operations (Marine Safety) Act 1994;*
- *Transport Operations (Passenger Transport) Act 1994; and*
- *Transport Operations (Road Use Management) Act 1995*.

The amendments to the *Transport Operations (Road Use Management) Act 1995, Transport Operations (Marine Safety) Act 1994, Transport Operations (Passenger Transport) Act 1994,* and the *Tow Truck Act 1973* (the 'transport Acts') will enable the Minister to replace current laminated products with a range of new smartcard products, as administered by the chief executive. The smartcard products to be introduced are—

- Driver Licence;
- Marine Licence Indicator;
- Bus, Taxi, Limousine, Motorcycle Tourist;
- Dangerous Goods;
- Tow Truck Driver;
- Tow Truck Assistant;
- Driver Trainer/Rider Trainer;
- Pilot/Escort Vehicle Driver; and
- Traffic Controller.

Short Title

The Short title of the Bill is the Transport (New Queensland Driver Licensing) Amendment Bill 2008.

Policy Objectives of the Legislation

Objectives of the Bills

The objectives of the Transport (New Queensland Driver Licensing) Amendment Bill 2008 are to amend the *Transport Operations (Road Use Management) Act 1995* in conjunction with amendments to the *Transport Operations (Marine Safety) Act 1994,* the *Transport Operations (Passenger Transport) Act 1994* and the *Tow Truck Act 1973* to allow for the—

- introduction of a range of new smartcard products (for example the new Queensland driver licence);
- capture and storage of digital photos and digitised signatures; and
- access and release of electronically stored information.

Reasons for the Bills

The New Queensland Driver Licence initiative represents the Queensland Government's response to a rapidly ageing technology for the issue of driver licences and other authorities. The current laminated products issued by Queensland Transport are vulnerable to fraud and their use to facilitate identity deceptions is on the increase. The current incidence of identity fraud and other criminal activity using falsely-obtained driver licences is unacceptably high, and is one of the main drivers for the Queensland Government's decision to introduce the new Queensland smartcard driver licence and associated industry licensing products.

For the first time Queensland Transport will take and store digital photos and digitised signatures of Queensland licence holders. With this, Queensland Transport will introduce digital photographic and facial recognition technology to confirm the applicant's identity for new, renewed or replacement driver licence products. To protect the personal information stored on the smartcard, the Queensland Government's *Information Standards IS42* (Information Privacy) and *IS18* (Information Security) have been used throughout the development of the smartcard platform.

As a result, it has been necessary to amend the *Police Powers and Responsibilities Act 2000* to—

- enable police to obtain an access approval order from a justice for a digital photo kept by Queensland Transport for the investigation, enforcement or prosecution of criminal law;
- enable police officers to access digital photos kept by Queensland Transport in specified emergency circumstances and for this access to be later authorised under a post-access approval order;
- authorise access by a police officer to information stored electronically on a smartcard for exercising a power under a transport Act or section 328A of the Criminal Code (dangerous operation of a vehicle);
- restrict the use of a photo or information to the purpose for which it was obtained; and
- require the destruction of photos in the presence of a justice.

Additional legislative amendments are required to the *Transport Operations (Road Use Management) Act 1995* (TORUM) to address the issues relating to outdated technology (current laminated products), identity fraud and information security. For consistency, amendments have been mirrored, where applicable, in the related transport Acts. Specifically, the amendments relate to—

- allowing for the collection and storage of digital photos and digitised signatures for the purposes of driver licensing;
- including new provisions to manage access to biometric data (stored on the department's Image Management System database) and other information about licence holders stored in the department's register;
- provisions that manage access to the information stored on the smartchip including information stored by the cardholder;
- providing for the cardholder to place non-licensing information on the smartchip;
- creating sanctions that are specific to the new smartcard; and
- providing for a parliamentary report of access by police to the digital photos.

Further to this, and to accommodate advances in electronic service delivery and the new National Document Verification Service (DVS) amendments have been included to allow—

(a) a person to give electronic consent for the release of information;

(b) instant verification of a person's documents should they use them as identity products (DVS); and

(c) the release of de-identified text data for road research purposes. De-identified data does not contain information that would allow a researcher to identify individual clients.

Also legislative amendments are required to the *Tow Truck Act 1973* to allow for a driver's certificate and assistant's certificate to take the form of a card. Specifically, the amendments are intended to—

- be in line with TORUM to include provision for the restricted access to digital photos and digitised signatures collected for the purposes of identifying a person gaining or renewing a certificate or an authority to operate a tow truck or operate as a tow truck operator's assistant;
- create a head of power to allow for a driver's certificate or assistant's certificate to take the form of a card or something similar, a PIN to be used as a security measure and verification of a person's identity for security purposes; and
- include sanctions that are specific to the new smartcard.

Also legislative amendments are required to the *Transport Operations (Marine Safety) Act 1994* to allow for Recreational Marine Driver Licences and Personal Watercraft Licences (proof of authority) to take the form of a card. Specifically, the additional amendments are intended to—

- be in line with TORUM to include provisions for the restricted access to digital photos and digitised signatures collected for the purposes of identifying a person gaining or renewing a marine licence indicator;
- create a specific head of power for a marine licence indicator to take the form of a card or something similar, a PIN to be used as a security measure and verification of a person's identity for security purposes; and
- include sanctions that are specific to the new smartcard.

Also legislative amendments are required for the *Transport Operations (Passenger Transport) Act 1994,* to allow for industry authorities to take the form of a card. Specifically, the amendments are intended to—

- be in line with TORUM to include provisions for the restricted access to digital photos and digitised signatures collected for the purposes of identifying a person gaining or renewing an authority for a taxi,

limousine service, a bus service, a tourist service or public passenger service;

- create a head of power to allow for a driver authorisation to take the form of a card or something similar, a PIN to be used as a security measure and verification of a person's identity for security purposes; and
- include sanctions that are specific to the new smartcard.

Achievement of Objectives

The Bill achieves its objectives in relation to Queensland's Information Privacy Principles by—

- incorporating the recommendations of the Crime and Misconduct Commission's 2005 report in the amended legislation to ensure that the section of the *Transport Operations (Road Use Management) Act 1995* that deals with the release of information does not apply to digital photos and digitised signatures;
- amending the *Police Powers and Responsibilities Act 2000* to allow for the implementation of a three tiered system for access and release of information from the department's Image Management System database;
- amending the *Transport Operations (Road Use Management) Act 1995*, *Transport Operations (Marine Safety) Act 1994*, *Transport Operations (Passenger Transport) Act 1994*, and the *Tow Truck Act 1973* to support a client transaction, by confirming the validity of a driver licence, where a client has chosen to use their driver licence as proof of identity in a non-driving situation;
- amending the *Transport Operations (Road Use Management) Act 1995*, *Transport Operations (Marine Safety) Act 1994*, *Transport Operations (Passenger Transport) Act 1994*, and the *Tow Truck Act 1973* to allow clients to release their driver licensing information through the use of the new Document Verification Service, for verification;
- amending the *Transport Operations (Road Use Management) Act 1995* to allow "de-identified" data to be provided to researchers that are contracted by Queensland Transport to undertake road safety related research on Queensland Transport's behalf;

- mirroring the new provisions, where applicable, in the *Transport Operations (Marine Safety) Act 1994*, *Transport Operations (Passenger Transport) Act 1994* and the *Tow Truck Act 1973*; and
- establishing a mechanism for a justice to oversee access outside the purpose of investigating, prosecuting and enforcing offences under the *Police Powers and Responsibilities Act 2000* and related road, traffic or transport Acts.

Alternatives to the Bill

The policy objectives require legislation to give them ongoing effect.

Estimated Cost for Government Implementation

It is not anticipated that the Queensland Government will face any administrative costs associated with the implementation of the proposed amendments as it will be conducted on a cost recovery basis.

Consistency with Fundamental Legislative Principles

The Bill has been drafted with due regard to the Fundamental Legislative Principles as outlined in the *Legislative Standards Act 1992*.

The Bill may breach the fundamental legislative principle relating to the right to privacy of an individual because of the retention of photos and signatures. However, the legislation contains safeguards that restrict access to photos and signatures and their use to specified purposes.

These safeguards include restricting access to digital photos—

- to the person whose facial image is on the photo, or someone else with that person's consent;
- to a police officer performing a function under a transport Act or section 328A of the Criminal Code; and
- to a police officer authorised to access a photo under an access approval order or a post-access approval under the *Police Powers and Responsibility Act 2000.*

Consultation

The following Government Departments and agencies were consulted on the development of the Bill—

- Department of the Premier and Cabinet;
- Queensland Treasury (Office of Liquor, Gaming and Racing);

- Queensland Police Service;
- Office of Queensland Parliamentary Counsel; and
- Department of Justice and the Attorney-General.

The Crime and Misconduct Commission has also been consulted throughout the development of the Bill.

Part 1 Preliminary

Clause 1 sets out the name (also called Short title) of the proposed Act.

Clause 2 provides for the commencement of the proposed Act on a day to be fixed by proclamation.

Part 2 Amendment of *Police Powers and Responsibilities Act 2000*

Clause 3 provides for the amendment of the *Police Powers and Responsibilities Act 2000*.

Clause 4 provides for the amendment of the Chapter 7 heading to include after 'documents,' 'accessing registered digital photos and other information'.

Clause 5 provides for the insertion of a new Part 5A 'Accessing registered digital photos and other information'. This clause sets out five new divisions and twelve new sections—

Division 1 Preliminary

Section 195A defines terms such as *access approval order*, *adult proof of age card*, *prescribed document* and *smartcard transport authority.*

Division 2 Access approval order for registered digital photo

Section 195B sets out when a police office considers it reasonably necessary to access a registered digital photo and the application process for an access approval order.

Section 195C sets out making the access approval order.

Section 195D sets out what the access approval order authorises.

Division 3 Accessing registered digital photo in an emergency

Section 195E sets out when a police officer can access a registered digital photo in an emergency. An emergency could be that police:

- reasonably suspect that there is an actual or imminent serious risk to a person's life or health or to public health or safety; and
- reasonably believe that immediate access of a particular person is likely to enable police to take action to reduce the risk. Section 195F sets out that a police officer who accesses a registered digital photo in an emergency must apply for a post-access approval order as soon as reasonably practicable after accessing the registered digital photo and the application process.

Section 195F sets out that a police officer who accesses a registered digital photo in an emergency must apply for a post-access approval order as soon as reasonably practicable after accessing the registered digital photo and the application process.

Section 195G sets out making the post-access approval order and that the justice is satisfied that police had the suspicion and belief required to access the photo and that there was no other way to obtain a current photo of the person who photo was accessed.

Section 195H sets out the appeal process where a justice has refused to make a post-access approval order.

Division 4 Accessing information stored electronically on a smartcard transport authority

Section 195I sets out that a police officer may access information stored electronically on a prescribed document without the consent of the cardholders for the purpose of exercising a power under a prescribed transport Act or in relation to the Criminal Code section 328A. A police officer may access emergency contact information stored electronically on the prescribed document without the consent of the cardholder if the police officer reasonably believes that there is an immediate risk to the holder's life or health or the person has died and a person with or near the holder is a person whom the police officer reasonably believes is a minor and a dependant of the holder and because of the attribute unable to give the police officer emergency contact details.

Division 5 Other provisions about accessing registered digital photos and other information

Section 195J requires the commissioner to give a copy of an access approval order or a post-access approval order to the relevant entity as soon as practicable after an order is made.

Section 195K declares that a police officer may only use a registered digital photo or information stored electronically on a smartcard transport authority for the purpose for which the access was allowed.

Section 195L requires a police officer to destroy the registered digital photo after it is no longer required for the purpose for which it was accessed, and that the destruction must be carried out in the presence of a justice.

Clause 6 provides for the amendment of Schedule 6 Dictionary to include definitions such as *access approval order* and *emergency contact information*.

Part 3 Amendment of *Tow Truck Act 1973*

Clause 7 provides for the amendment of the *Tow Truck Act 1973*.

Clause 8 provides for an insertion of a new heading 'Division 1 General' within Part 3.

Clause 9 provides for an insertion, after section 19, of two new divisions and eight new sections—

Division 2 Biometric data and other information relating to driver's certificate or assistant's certificate

Section 19A requires an applicant for a driver's certificate or assistant's certificate to allow the chief executive to take and keep a digital photo and digitised signature and sets out the other ways in which a digital photo and digitised signature can be obtained for their use on a card.

Section 19B sets out the purposes for which digital photos and digitised signatures can be used. This includes—

- verifying a person's identity for the issuing of a relevant certificate;
- the reproduction of digital photos and digitised signatures on a relevant certificate;
- verifying a person's identity for the security features, such as setting a PIN; and
- for the investigation and prosecution of an offence under the Act.

Section 19C imposes restrictions on the access of digital photos. The chief executive may give a cardholder access to a photo if the person's facial image is encoded on the digital photo and the person's connection to the photo is established by facial recognition technology or some other evidence of the person's identity. A police officer must be granted access for exercising a power under the Act, or the Criminal Code section 328A or where the access is authorised under the *Police Powers and*

Responsibilities Act 2000. Access means obtaining a copy of the digital photo, including by electronic communication.

Section 19D requires the chief executive to ensure that digital photos and digitised signatures are deleted from any register or similar record kept when their retention period has ended.

Section 19E restricts access to information stored electronically on a smartcard certificate to—

- the holder or someone with the holder's consent; or
- a police officer authorised under the *Police Powers and Responsibilities Act 2000*; or
- a person authorised under this Act.

Access includes viewing or taking a copy of the information. This section also provides for an offence for non-compliance and imposes a penalty of 20 penalty units.

Section 19F provides that the retention period for a digital photo or digitised signature is 30 years. However the section provides for different periods in particular circumstances and the method for working out the retention period.

Section 19G obliges the chief executive to provide an annual report regarding access by police officers under section 19C to digital photos kept on the register. A report will be tabled by the Minister before the Legislative Assembly that shows what access the police have had to the register.

Division 3 Restricted release of information about driver's certificate or assistant's certificate

Section 19H provides that the chief executive may release information kept under the Act about a person's driver certification or assistant's certificate to the person, or with the person's written consent another person, the commissioner of the police service or, another entity. The chief executive may release information to an entity if the person produces the certificate to the entity as proof of identity and the entity applies in the approved form and the information is necessary to verify the validity of the certificate.

The information that may be released does not include a digital photo and digitised signature. The provision also allows that an application may be made by electronic communication.

Clause 10 amends section 36C (Confidentiality) to extend the term information to include digital photo and digitised signature.

Clause 11 amends section 43 which is the regulation-making power to allow a regulation to be made to provide that a driver's certificate or assistant's certificate may take the form of a card on which information may be stored electronically, a PIN number to be used as a security measure and to verify a person's identity for security purposes.

Clause 12 provides for the amendment of Schedule 2 Dictionary to include definitions such as *electronic communication*, *prescribed smartcard Act*, and *retention period*.

Part 4 Amendment of *Transport Operations (Marine Safety) Act 1994*

Clause 13 provides for the amendment of the *Transport Operations (Marine Safety) Act 1994*.

Clause 14 amends section 62 (grant, amendment and renewal of licences) to allow a regulation to be made for a marine licence indicator to take the form of a card on which information may be stored electronically, a PIN number to be used as a security measure and to verify a person's identity for security purposes.

Clause 15 provides for the insertion of two new divisions and nine new sections—

Division 3A Biometric data and other information relating to marine licences

Section 63A requires an applicant for a marine licence to allow the chief executive to take and keep a digital photo and digitised signature and sets

out the other ways in which a digital photo and digitised signature can be obtained for their use on a card.

Section 63B sets out the purposes for which digital photo's and digitised signatures can be used. This includes—

- verifying a person's identity for the issuing of a marine licence;
- the reproduction of digital photos and digitised signatures on a marine licence indicator;
- verifying a person's identity for the security features, such as setting a PIN; and
- the investigation and prosecution of an offence under the Act.

Section 63C imposes restrictions on the release of digital photos. The chief executive may give a cardholder access to a photo if the person's facial image is encoded on the digital photo and the person's connection to the photo is established by facial recognition technology or some other evidence of the person's identity. A police officer must be granted access for exercising a power under the Act, or the Criminal Code section 328A, or where the access is authorised under the *Police Powers and Responsibilities Act 2000*. Access means obtaining a copy of the digital photo, including by electronic communication.

Section 63D obliges the chief executive or general manager to ensure that digital photos and digitised signatures are deleted from any register or similar record kept when their retention period has ended.

Section 63E provides for a cardholder's emergency contact information to be stored electronically on a smartcard marine licence indicator

Section 63F restricts access to information stored electronically on a smartcard marine licence indicator to—

- the holder or someone with the holder's consent; or
- a police officer authorised under the *Police Powers and Responsibilities Act 2000*; or
- a person authorised under another Act, however this person must not access Emergency Contact Information

Access includes viewing or taking a copy of the information. This section also provides for an offence for non-compliance and a fine of 20 penalty units.

Section 63G provides that the retention period for a digital photo or digitised signature is 30 years. However, the section provides for different periods in particular circumstances and the method for working out the retention period.

Section 63H obliges the chief executive to provide an annual report that relates to access made by police officers under section 63C to digital photos kept on the register. A report will be tabled by the Minister before the Legislative Assembly that will provide a record of police access to the register.

Division 3B Restricted release of information about marine licences

Section 63I provides that the chief executive may release information kept under the Act about a person's marine licence:

- the person; or
- with the person's written consent another person; or
- the commissioner of the police service; or
- another entity.

The chief executive may release information to an entity if

- the person produces the marine licence to the entity as proof of identity; and
- the entity applies in the approved form; and
- the information is necessary to verify the validity of the marine licence indicator.

The information that may be released does not include a digital photo and digitised signature. The provision also allows an application to be made by electronic communication.

Clause 16 replaces section 205AC to include a broader confidentiality provision.

Clause 17 provides for the amendment of the Dictionary to include definitions such as *electronic communication*, *emergency contact information*, and *prescribed smartcard Act*.

Part 5 Amendment of *Transport Operations (Passenger Transport) Act 1994*

Clause 18 provides for the amendment of the *Transport Operations (Passenger Transport) Act 1994*.

Clause 19 provides for a new heading Part 1 General.

Clause 20 amends section 29 (Granting, renewing or refusing driver authorisation) to allow a regulation to be made for a driver authorisation to take the form of a card on which information may be stored electronically, a PIN number to be used as a security measure and to verify a person's identity for security purposes.

Clause 21 inserts a new section 34A (Authorised driver must notify loss, theft, damage or destruction of driver authorisation) that requires a driver authorisation holder to notify the chief executive if the holder's card is lost, stolen damaged or destroyed and provides for an offence for non-compliance.

Clause 22 provides for the insertion of a new Part 2 'Biometric data and other information relating to driver authorisation' and Part 3 'Restricted release of information about driver authorisation'. This clause sets out two new parts and eight new sections—

Part 2 Biometric data and other information relating to driver authorisation

Section 35A requires an applicant for a driver authorisation to allow the chief executive to take and keep a digital photo and digitised signature. This section also sets out the other ways in which a digital photo and digitised signature can be obtained for their use on a card.

Section 35B sets out the purposes for which digital photo's and digitised signatures can be used. This includes—

- verifying a person's identity for the issuing of a driver authorisation;

- the reproduction of digital photos and digitised signatures on a driver authorisation;
- verifying a person's identity for the security features, such as setting a PIN; and
- the investigation and prosecution of an offence under the Act.

Section 35C imposes restrictions on the release of digital photos. The chief executive may give a cardholder access to a photo if the person's facial image is encoded on the digital photo and the person's connection to the photo is established by facial recognition technology or some other evidence of the person's identity. A police officer must be granted access for exercising a power under the Act, or the Criminal Code section 328A, or where the access is authorised under the *Police Powers and Responsibilities Act 2000*. Access means obtaining a copy of the digital photo, including by electronic communication.

Section 35D obliges the chief executive to ensure that digital photos and digitised signatures are deleted from any register or similar record kept when their retention period has ended.

Section 35E restricts access to information stored electronically on a smartcard driver authorisation to—

- the holder or someone with the holder's consent; or
- a police officer authorised under the *Police Powers and Responsibilities Act 2000*; or
- a person authorised under this Act.

Access includes viewing or taking a copy of the information. This section also provides for an offence for non-compliance and a fine of 20 penalty units.

Section 35F provides that the retention period for a digital photo or digitised signature is 30 years. However, the section provides for different periods in particular circumstances and the method for working out the retention period.

Section 35G obliges the chief executive to provide an annual report that relates to police access under section 35C to digital photos kept on the register. A report will be tabled by the Minister before the Legislative Assembly that will provide a record of police access to the register.

Part 3 Restricted release of information about driver authorisation

Section 35H sets out that the chief executive may release information kept under the Act about a person's driver authorisation

- to the person; or
- with the person's written consent another person; or
- the commissioner of the police service; or
- another entity.

The chief executive may release information to an entity if

- the person produces the driver authorisation to the entity as proof of identity; and
- the entity applies in the approved form; and
- the information is necessary to verify the validity of the driver authorisation.

The information that may be released does not include a digital photo and digitised signature. The provision also allows an application to be made by electronic communication.

Clause 23 amends section 148C (Confidentiality) to include the term information which includes digital photo and digitised signature.

Clause 24 provides for the amendment of Schedule 3 Dictionary to include definitions such as *electronic communication*, and *prescribed smartcard Act*.

Part 6 Amendment of *Transport Operations (Road Use Management) Act 1995*

Clause 25 provides for the amendment of the *Transport Operations (Road Use Management) Act 1995*.

Clause 26 amends section 77 to allow the chief executive to verify to another entity a person's prescribed authority and to prevent the release of digital photos and digitised signatures under section 77.

Clause 27 inserts a new section 77A that provides for de-identified information to be released for statistical road research purposes.

Clause 28 provides for an insertion of a new Part 3A Biometric data and other information relating to prescribed authority holders. This clause inserts eight new sections—

Part 3A Biometric data and other information relating to prescribed authority holders

Section 91A requires an applicant for a prescribed authority to allow the chief executive to take and keep a digital photo and digitised signature. This section also sets out the other ways in which a digital photo and digitised signature can be obtained for their use on a card.

Section 91B sets out the purposes for which digital photos and digitised signatures can be used. This includes—

- verifying a person's identity for the issuing of a prescribed authority;
- the reproduction of digital photos and digitised signatures on a prescribed authority;
- verifying a person's identity for the security features, such as setting a PIN; and
- the investigation and prosecution of an offence under the Act.

Section 91C imposes restrictions on the release of digital photos. The chief executive may give a cardholder access to a photo if the person's facial image is encoded on the digital photo and the person's connection to the photo is established by facial recognition technology or some other evidence of the person's identity. A police officer may be granted access for exercising a power under the Act, or the Criminal Code section 328A, or where the access is authorised under the *Police Powers and*

Responsibilities Act 2000. Access means obtaining a copy of the digital photo, including by electronic communication.

Section 91D obliges the chief executive to ensure the digital photos and digitised signatures are deleted from any register or similar record kept when their retention period has ended.

Section 91E provides for a cardholder's emergency contact information to be stored electronically on a smartcard driver licence.

Section 91F restricts access to information stored electronically on a smartcard driver licence to—

- the cardholder or someone with the cardholder's consent; or
- a police officer authorised under the *Police Powers and Responsibilities Act 2000*; or
- a person authorised under this Act, however this person must not access Emergency Contact Information.

Access includes viewing or taking a copy of the information. This section also provides for an offence for non-compliance and a fine of 20 penalty units.

Section 91G provides that the retention period for a digital photo or digitised signature is 30 years. However, the section provides for different periods in particular circumstances and the method for working out the retention period.

Section 91H obliges the chief executive to provide an annual report that relates to access made by police officers under section 91C to digital photos kept on the register. A report will be tabled by the Minister before the Legislative Assembly that will provide a record of police access to the register.

Clause 29 amends section 143 (Confidentiality) to extend the definition of information to include a digital photo and digitised signature.

Clause 30 amends section 150A (Regulating form of licence) to allow a regulation to authorise a prescribed authority to be in the form of a card on which information may be stored electronically, a PIN number to be used as a security measure and to verify a person's identity for security purposes.

Clause 31 provides for the amendment of Schedule 4 Dictionary to include definitions such as *digital photo*, *digitised signature*, *electronic communication*, *emergency contact information*, and *retention period*.