2011

THE LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

ROAD TRANSPORT (SAFETY AND TRAFFIC MANAGEMENT) AMENDMENT BILL 2011

SUPPLEMENTARY EXPLANATORY STATEMENT

Circulated by authority of
Simon Corbell MLA
Attorney-General

Supplementary Explanatory Statement –

These amendments are circulated under Standing Order 182A on the basis that they are urgent.

Outline of amendments

The first amendment provides for the deletion of stored images held on the cameras in a point to point system, no later than 30 days after they are taken. Images are stored on the camera to provide sufficient time for processing by the Traffic Camera Office and for access by ACT Policing, if an image is required in relation to a criminal investigation. These issues are explained in more detail in the clause notes for this amendment.

The second set of amendments address concerns about the operation and breadth of proposed new sections 29 and 29A in clause 27 of the Bill. The amendments set out the permitted primary and secondary purposes for using and disclosing images, ensures that there are appropriate restrictions relating to the use, retention and subsequent disclosure of images that are disclosed to other persons, and requires the road transport authority and other persons to whom images are disclosed to implement safeguards to protect those images. These provisions, and issues relating to their operation, are discussed in greater detail in the clause notes. The level of detail in the discussion of some matters reflects requests for further information about some matters following presentation of the Bill.

Notes on Clauses

Government Amendment 1

New clause 15A New section 24 (3)

This clause will insert new section 24 (3) into the Act. Section 24 is a regulation making power. Under the Act, an average speed detection system is approved for use if a regulation is made to prescribe its use in the ACT. New section (3) makes it clear that a regulation cannot approve an average speed detection system unless that system ensures that the images taken by the cameras at each of the detection points in the system are deleted from those cameras no later than 30 days after they were taken. This will enable sufficient time for images that disclose a speeding offence to be transferred from the cameras to the Traffic Camera Office for adjudication and preparation of infringement notices, including sufficient time to re-send the images in the event of a transmission failure or another technical problem affecting either the hardware or software in the matching server, the adjudication system within the Traffic Camera Office or the storage server for traffic infringements maintained by InTACT. 30 days is also regarded as a sufficient period for ACT Policing to request and obtain an image that may be 'reasonably necessary' in connection with a criminal investigation, as permitted by proposed new sections 29A (b).

It should be noted that images that are used in relation to infringement notices for a speeding offence are required to be held for 7 years under the *Territory Records Act 2002.* Images disclosed to ACT Policing in connection with other criminal

investigations will be held for as long as reasonably required for that purpose - depending on whether the investigation results in a trial, that period of time may be several years, allowing for any appeals to be finalised.

Government Amendment 2

Clause 27 New sections 29 to 29C

This item replaces clause 27 of the Bill with a new clause 27, containing proposed new sections 29 to 29C.

The purpose of these sections is to regulate the way in which images from traffic cameras may be used and disclosed. These provisions apply a standard of protection to images which is more restrictive than that which applies to 'personal information' under the *Privacy Act 1988*. These amendments are included because the images, by themselves, are considered not to be 'personal information' information within the meaning of the *Privacy Act 1988*.

The reason that images are considered not to be 'personal information' is that the existing camera technology focuses on the numberplate region of cars; the images by themselves are not useful in identifying the registered operator or driver of the vehicle. Unless and until the image has been linked with information in the registration database, it is not possible for someone to view the image and identify the registered operator of the vehicle, or to identify the driver - noting of course that the registered operator and the driver may not be the same person.

However, it is conceivable that in the future, the camera technology used in the ACT traffic camera program might change, enabling facial recognition. Where a driver's identity could be discerned from an image, the image could become 'personal information' within the meaning of the *Privacy Act 1988*.

It should be noted that the adoption of facial recognition cameras would require a departure from the existing preference for taking images of the rear of vehicles, wherever this is practicable. This policy exists because motorcycles only display numberplates on the rear of the vehicle, for safety reasons. Motorcycle safety, including speed management for motorcyclists, is a significant road safety issue in the ACT and nationally.

There are no plans for the implementation of technology in the TCO which would enable facial recognition. It will be for future governments, with guidance from future Assemblies, to determine whether facial recognition technology is appropriate for the ACT traffic camera program.

There are also obligations on public officers in relation to the use and disclosure of official information, whether the official information is also 'personal information' or otherwise, that arise under section 9 of the *Public Sector Management Act 1994*. There is an offence relating to the unauthorised use or disclosure of information by public officials in section 153 of the *Crimes Act 1900*, which they have a duty not to use or disclose. The duty in this instance would arise under new sections 29 and 29A, and also under section 9 of the *Public Sector Management Act 1994*. In

addition, there are offences relating to unauthorised access to restricted computer databases under section 420 of the *Criminal Code 2002,* noting that access the traffic cameras, the matching server and the databases used by the Traffic Camera Office is 'restricted' within the meaning of that section.

New section 29 sets out the purposes for which images from cameras may be used. It makes clear the primary purpose for using these images is the enforcement of traffic offences under the road transport legislation (proposed section 29 (a)).

Section 29 also recognises that there may be secondary purposes for which the images may be used, and these are listed in paragraphs (b) and (c). It is not unusual for legislation that provides for the collection of information for one purpose to permit that information to be used for other purposes. For example, Information Privacy Principles (IPP) 10 and 11, National Privacy Principle 2 under the *Privacy Act 1988*, and Health Information Privacy Principles (HIPP) 9 and 10 under the *Health Records (Privacy and Access) Act 1997*, all list the secondary purposes for which personal information may be used.

New section 29 (b) will allow images to be used where reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty. The purpose in section 29 (b) reflects the purpose in IPP 10.1(d), but it is more restrictive than IPP 10.1(d) because it does not include a reference to the protection of public revenue. IPP 10.1(d) recognises that the enforcement of the criminal law is a legitimate secondary purpose for using information collected and held by government agencies.

Guideline 39 of the *Plain English Guidelines to the Information Privacy Principles*, issued by the Privacy Commissioner[1] explains the following in relation to the "law enforcement purpose" in IPP 10.1 (d) and 11.1(e):

> *"Criminal law" means any Commonwealth, State, or Territory law that makes particular behaviour and offence punishable by fine or imprisonment. Broadly speaking, "criminal law" encompasses those laws that make an act a crime, so that criminal proceedings can be taken. These proceedings are usually prosecuted by the police or Crown prosecutors. They are usually heard in criminal courts, and may result in the accused being convicted and punished by fine or imprisonment.*
>
> ***Criminal law of non-Australian jurisdictions***
> *"Criminal law" may include the law of non-Australian jurisdictions if the Commonwealth agrees to it under the Mutual Assistance in Criminal Matters Act. But an agency may more appropriately seek to justify a use or disclosure to enforce this kind of law by using exception 10.1(c) or 11.1(d).*
>
> ***Meaning of "to enforce" the criminal law***
> *"To enforce" the criminal law means:*
> - *the process of investigating crime and prosecuting criminals, and*

[1] The Guidelines are available, in three parts, at http://www.privacy.gov.au/materials/types/guidelines.

- *gathering intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies.*

Who can disclosures be made to?

An agency should only disclose personal information that is reasonably necessary to enforce the criminal law, to:

- *an organisation that has statutory responsibilities for investigating or prosecuting criminal offences*
- *person or organisation that must be told the personal information so that they can help in the investigation or prosecution.*

Examples of permissible uses and disclosures

These are examples of uses and disclosures that are reasonably necessary to enforce the criminal law, within exceptions 10.1(d) and 11.1(e):

- *An agency may disclose relevant personal information to a State Department of Corrective Services that is trying to decide where to imprison people convicted of criminal offences.*
- *Police may disclose personal information - for example, the identity of an offender - if the disclosure is necessary for the criminal compensation system to function."*

It is considered that section 29 (b), which is consistent with IPP 10.1(d), is a reasonable limitation on the right to privacy for the purpose of section 28 of the *Human Rights Act 2004.*

The purpose in new section 29 (c) reflects IPP 10.1(c) and HIPP 9 (1) (e). In summary, it provides for the use of images where the use is required or authorised by law. Guidelines 32 to 34 of the *Plain English Guidelines to the Information Privacy Principles* discuss what is meant by "law" (Guideline 32), "required by" (Guideline 33) and "authorised by" (Guideline 34) and may assist in the interpretation and operation of new section 29 (c) and new section 29A (c). A "law" for this purpose will include Commonwealth laws, Territory laws (at least in so far as the agency concerned is a Territory agency), an order of a court, directions or orders made pursuant to Commonwealth Parliamentary privilege, and may include certain instruments that have the force of law such as industrial awards.[2]

The actual wording of new section 29 (c), and also new section 29A (c), is modelled on HIPP 9 (1) (e) rather that the IPPs, because it is believed that the HIPP wording more clearly articulates the concept of 'law' and is therefore more accessible to readers of the legislation. The HIPP wording differs from the wording used in IPP 10 and 11 because it clearly identifies the sources of the relevant 'law' under which the requirement or authorisation occurs. These sources are:

- laws of the Commonwealth
- laws of the Territory
- orders of a court of competent jurisdiction.

This formulation may be very slightly narrower than the formulation used in IPPs 10 and 11, because it does not cover a use or disclosure that is required or authorised

[2] Plain English Guidelines to the Information Privacy Principles (IPPS 8 to 11), at pages 40 to 41.

by a law of a State[3], or the common law, and does not cover Commonwealth Parliamentary privilege.

Guideline 33 of the *Plain English Guidelines to the Information Privacy* deals with the concept of a use 'required by or under law':[4]

> **"*When does a law require an agency to use information for another purpose?***
>
> *A use for another purpose is usually required by law if legislation governing the using agency specifically requires it to use the personal information for a purpose different from that for which it is obtained.*
>
> *An agency may also be required by law to use personal information for another purpose if:*
> - *the agency is governed by legislation that requires it to perform a specific function, and*
> - *the only possible way the agency can perform that function is by using the particular information for a purpose different from that for which it was obtained.*

In relation to what is meant by a use 'authorised by or under law", Guideline 34 of the *Plain English Guidelines to the Information Privacy Principles* explains:[5]

> *A use for another purpose is a use for a purpose different from that for which the personal information is obtained. A law authorises a use for another purpose if legislation governing the using agency clearly and specifically gives it a discretion to use the personal information for that purpose. The agency must be able to point to a specific relevant discretion in the legislation governing it.*
>
> *A use is not authorised (within 10.1(c)) by a section in an Act that gives a public office holder a general discretion "to do any thing necessary or convenient to be done for or in connection with" their functions. A use is also not authorised just because there is no law prohibiting it. If it were, almost any use would be authorised by law and IPP 10.1 would be ineffective."*

It is noted that the type of use permitted by section 29 (c) is consistent with existing standards of privacy protection for 'personal information", and is restricted to legitimate purposes properly authorised or required by law. It is therefore considered that the impact of section 29 (c) on the right to privacy would be a reasonable limitation of that right for section 28 of the *Human Rights Act 2004*.

---

[3] The Guidelines state at page 40: "*Where a State/Territory has validly legislated to bind the Commonwealth, these State/Territory laws are also considered 'law'. The question of whether a State/Territory has validly legislated to bind the Commonwealth is often a complex one. It is therefore advisable for a commonwealth agency to seek legal advice if unsure whether it is bound by State/Territory law in the given circumstances."*

[4] Guidelines, page 42.

[5] Guidelines, page 42.

It should be noted that if a future Assembly wished to use camera images for a purpose other than a purpose already covered by section 29, it would be necessary to legislate to permit that use. A statement of compability under the *Human Rights Act 2004* would be required for that future legislation.

New section 29A is similar in structure to new section 29, but applies to the disclosure of images rather than their use.

New section 29A (a) provides for the disclosure of images in connection with the enforcement of the road transport legislation. This is the primary purpose for which images are collected under the legislation. For example, images would need to be disclosed to police and prosecution authorities and to the Courts in connection with a prosecution for a speeding or red light offence. Images may also need to be disclosed to external contractors who maintain and service the cameras.

New section 29A (b) provides for the disclosure of images where reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty. The purpose in section 29A (b) reflects the purpose in IPP 11.1(e), but it is slightly more restrictive than IPP 11.1(e) because it does not include a reference to the protection of public revenue.

IPP 11.1(e) recognises that the enforcement of the criminal law is a legitimate secondary purpose for disclosing information collected and held by government agencies. It is understood that police in other Australian jurisdictions with traffic camera programs, including 'human rights' jurisdictions such as Victoria and in the United Kingdom, are allowed to access and/or use images in connection with the investigation of other criminal offences. It is considered that section 29A (b), which is consistent with IPP 11.1.(e) and reflects the practice in other jurisdictions with human rights legislation, is a reasonable limitation on the right to privacy for the purpose of section 28 of the *Human Rights Act 2004.*

The purpose in section 29A (c) reflects IPP 11.1(d) and HIPP 10 (2) (e) (disclosure required or authorised by law etc). In summary, it provides for the disclosure of images where the disclosure is 'required or authorised by law'. As previously explained in the clause notes for new section 29, the HIPP wording for the 'required or authorised by law' purpose has been adopted in preference to the IPP wording because it clearly states the sources of the 'law' under which the disclosure may be required or authorised. As with section 29 (c), this provision does not, of itself, authorise the disclosure – it operates only where that other law already has that effect. It is believed that this type of 'secondary purpose' disclosure is consistent with existing standards of privacy protection and that section 29A (c) is a reasonable limitation of the right to privacy for section 28 of the *Human Rights Act 2004*.

Guideline 33 of the *Plain English Guidelines to the Information Privacy Principles* explains when a law requires the disclosure of information:[6]

> *"An agency is required by law to disclose personal information if a law governing it specifically requires it to disclose information.*

[6] Guidelines, page 42.

For example: a law may require an agency to reveal relevant personal information to a review tribunal or to a person seeking a review of a decision. The agency must comply with this law _ although if the law also gives the agency a discretion to withhold specific information, it should exercise that discretion where appropriate.

An agency is also required by law to disclose personal information if:

- *legislation governing the agency to whom the information is to be disclosed (the "receiving agency") gives that agency power to require the specific information to be disclosed, and*
- *the receiving agency exercises its power to require the disclosure by formally advising the disclosing agency that it is exercising that power (for example, by issuing a notice to the disclosing agency).*

Guideline 34 of the *Plain English Guidelines to the Information Privacy Principles discusses when a disclosure may be authorised by a law:*[7]

"A law authorises a disclosure if legislation governing the disclosing agency clearly and specifically gives it a discretion to disclose the personal information.

The disclosing agency must be able to point to a specific relevant discretion in the legislation governing it. It is not enough for the receiving agency to show that the personal information is relevant to its lawful functions.

A disclosure is not authorised (within 11.1(d)) by a section in an Act that gives a public office holder a general discretion "to do any thing necessary or convenient to be done for or in connection with" their functions. This is the case whether the section applies to the disclosing or receiving agency.

If legislation governing a disclosing agency prohibits a disclosure, the agency cannot make that disclosure - even if legislation governing the receiving agency gives it a general discretionary authority to obtain the personal information.

A disclosure is not authorised by law just because there is no law prohibiting it. If it were, almost any disclosure would be authorised by law and IPP 11.1 would be ineffective."

An example of a disclosure that may be authorised by law may be a disclosure for the purpose of a disciplinary investigation into an allegation of unauthorised access to an image by a public servant or a police officer.

Disclosures required or authorised by an order of a court would include the production of an image pursuant to a subpoena or a warrant issued by a court. The type of subpoena that is used to require the production of a document was historically known as a *subpoena duces tecum*. This was a writ issued by a court

[7] Guidelines, page 43.

that required the person on whom it was served to attend the court, with specified documents, for use in a matter before the courts. It has its origins in the Courts of Chancery in England, and was gradually adopted by the common law courts.

In 1996, Justice Michael Kirby summed up the importance of the subpoena in these terms[8]:

> "*Without the subpoena, the rule of law gives way to the rule of power. The ordinary citizen, and even the courts, cannot command the powerful to submit to curial jurisdiction over disputed matters. In a report to the General Assembly of the United Nations I called specific attention to the need for the writ of subpoena. Its utility, taken for granted by Australian lawyers, is blindingly obvious in a society that does not have the facility available."*

A subpoena can only be issued by the court once the jurisdiction of the court has been enlivened by the initiation of a proceeding, either civil or criminal. In the ACT, the process for issuing and serving a subpoena is set out in the *Court Procedures Rules 2006.*

It should be noted other bodies exercising investigative and determinative functions may be invested by legislation with subpoena-like powers, that is, the power to compel witnesses to attend, give evidence and produce documents. For example, royal or judicial, commissions, boards of inquiry, the Australian Crime Commission and various regulatory boards and tribunals may be given these powers. A witness who fails to attend or produce the required document commits an offence.

Another type of court order that may result in the production or disclosure of a document is a warrant, including a search warrant. The *Crimes Act 1900* contains provisions for issuing search warrants (see Division 10.3 of that Act) in relation to evidential material for criminal investigations. Section 194 (1) of that Act permits an issuing officer to issue a search warrant to search premises if the officer is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises. It is presumed that a RTA traffic camera installation would be regarded as 'premises' for this purpose. Sections 199 and 200 of that Act deal with the use of electronic equipment to examine things at premises, and would be invoked to enable the officers executing the warrant to access images stored on the cameras.

Other ACT legislation also contains search warrant powers, usually in relation to specific categories of documents, things or information relevant to that legislation. For example, a medicines and poisons inspector may apply for a search warrant to enter premises under Division 7.1.4 of the *Medicines, Poisons and Therapeutic Goods Act 2008* to search for evidential material relevant to breaches of that act. Many of these search powers would not be relevant to images stored on traffic cameras managed by the road transport authority.

---

[8] The Hon Justice M D Kirby AC CMG, 1996: Forward to "Subpoena Law and Practice In Australia", Gerard B Carter http://www.michaelkirby.com.au/images/stories/speeches/1990s/vol36/1996/1325-Foreword_-_Subpoena_Law_and_Practice_in_Australia.pdf

It should be noted that if a future Assembly wished to use camera images for a purpose other than a purpose already covered by section 29A, it would be necessary to legislate to permit that use. A statement of compability under the *Human Rights Act 2004* would be required for that future legislation.

New section 29B applies to a person to whom an image has been disclosed under section 29A. It is intended to guard against the misuse of images by these people. It sets limits on the use that the person may make of the image. It also provides that person cannot retain the image for longer than is necessary for the purpose for which the disclosure was made, or longer than required by law – noting that some persons to whom images are disclosed, such as police or courts, may be subject to legal requirements to archive the images for a period of time.

Finally, it provides that the person cannot disclose the image to a third person, unless that subsequent disclosure is itself authorised or required by law. It should be noted that this provision does not of itself authorise any subsequent disclosure. Another law must do that if the disclosure is to be lawful. The purpose of section 29B (c) is to prevent any subsequent disclosure, except where that disclosure is required or authorised by another law.

For example, a police officer to whom an image is disclosed would ordinarily be authorised to include the image in a brief of evidence that is given to the court for a matter, and the prosecutor would be permitted to disclose the image to a senior counsel. It is appropriate to ensure that new section 29C does not operate to prevent a disclosure that another law has required or authorised, as this could undermine the effective operation of that other law contrary to the intention or expectation of the legislature.

New section 29C imposes an obligation on the road transport authority and other persons to whom images are disclosed to implement security measures to protect those images. This provision reflects the obligation under IPP 4 (1) in the *Privacy Act 1988*.

The Traffic Camera Office has implemented a range of security measures for its point to point camera systems. Data and images stored in each camera unit will be 1024-bit encrypted using a public key. Opening an encrypted file requires a private encryption key. The image file cannot be decrypted without that private 1024 bit key. The key is stored on a system to which only authorised personnel within the Traffic Camera Office will have access. The adjudication system will apply the private encryption key to enable the encrypted image files to be viewed and adjudicated. Adjudication staff will assess each set of images to determine whether an offence has been committed.

All data and timestamps on images are applied when images are captured, using a Stratum 1 time source (via a GPS receiver). Image files, even after they have been decrypted, cannot be altered by the Traffic Camera Office or anyone else.

Access to the data logs for the cameras will be controlled by existing whole-of-government ICT security protocols. These protocols will require that a person who seeks to access the logs must have access to the ACT Government network, to have a logon and password to access the server where the logs are maintained and to be logged onto a computer that has had its IP address pre-identified to the server. In practice, this access will be restricted to around four staff in the road transport authority who are responsible for managing the traffic camera program and maintaining this system.

At present, eleven staff in the Traffic Camera Office have access to the adjudication system. Access is controlled by existing whole of government ICT security protocols. All staff needing access to the database to perform their duties are required to read and sign a Deed of Confidentiality outlining their responsibilities under the *Privacy Act 1988* and for accessing and dealing with information managed by the RTA.

It should be noted that access to vehicle registration information, which may be linked to images after a speeding offence is detected, is also controlled. That information includes personal information within the meaning of the *Privacy Act 1988*, and staff who work with that information have obligations under that Act, as well as under section 9 of the Public Sector Management Act 1994, not to disclose it. The offences under section 153 of the *Crimes Act 1900* and section 420 of the *Criminal Code 2002* would apply in relation to unauthorised access to/use of information on the vehicle registration database.
