Chapter 7 Obtaining Information from External Bodies

7.1 State departments

7.1.1 Residential Tenancies Authority

The Residential Tenancies Authority (RTA) is only able to conduct searches and provide personal information under the provisions of a subpoena, search warrant or other compellable document (such as a direction under s. 7.15.9: 'Section 42 (Direction to government entity)' of the Operational Procedures Manual). See s. 527: 'Confidentiality' of the *Residential Tenancies and Rooming Accommodation Act*.

Generally, the RTA may hold personal information relating to a person's name, previous or current addresses and the duration of a tenancy. For more information on the types of information and documents that may be held by the RTA, see the 'RTA Warrants Information Sheet' available on Forms Select.

Officers must be aware any information provided by the RTA in response to a warrant has been provided by the party in question and not independently validated.

Processing the subpoena, search warrant or other order

To execute the search warrant, officers should email the RTA (see SMCD):

(i) the search warrant;

(ii) a Form 11: 'Statement to occupier'; and

(iii) the relevant completed search criteria template on the 'RTA Warrants Information Sheet'.

Warrants executed on the RTA will be processed and returned within 5 business days. The relevant information will be emailed back to the requesting officer.

7.1.2 Requesting go card information from TransLink

TransLink is a division of the Department of Transport and Main Roads (DTMR) responsible for the management of public transportation in a number of regions in Queensland. TransLink operate the *go* card pre-paid ticketing system.

This system allows members of the public to purchase and maintain a *go* card account for the electronic payment of fares on the public transport infrastructure. Users may register their personal details against their *go* card account.

TransLink retain journey and usage records of all registered and unregistered *go* cards. Officers may request *go* card account information from TransLink when investigating a criminal offence or to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.

Officers requiring specific *go* card account information are to ensure all Service information and intelligence have been exhausted before any request to TransLink is made.

ORDER

Requests for *go* card account information are to be made to TransLink on a F 4961: 'DTMR – Request for information' (available on Forms Select). The information is to contain sufficient detail for TransLink to satisfy itself under the provisions of the *Information Privacy Act* (IPA) and Information Privacy Principle 11.

Should the contents of the request contain information classified 'Highly Protected' (see s. 4.4.5.1.3: 'Highly Protected' of the Information Management Manual), a Detective Inspector, Crime and Intelligence Command shall engage with TransLink on behalf of the Service to negotiate the release of information and satisfy TransLink the request is in compliance with the IPA and Information Privacy Principle 11.

Officers requiring *go* card account information are to:

(i) complete a F 4961: 'DTMR – Request for information';

(ii) submit it for the approval of a senior officer (rank of sergeant or above);

(iii) if approved, forward the completed form to TransLink; and

(iv) scan and save the completed form in the relevant QPRIME occurrence.

Officers requiring CCTV footage from TransLink are to complete a F 4961 'DTMR – Request for information' (see s. 2.28.2: 'Obtaining video recordings from the Department of Transport and Main Roads' of the OPM).

7.1.3 Department of Agriculture and Fisheries, Fisheries Licensing Unit

The Queensland Fisheries, Department of Agriculture and Fisheries (DAF) (see SMCD) maintains a register of authorities and may issue certificates about authorities which are admissible in proceedings as evidence. A search of individual authorities may include a request for the licence details of a boat, a fisher or a sea food wholesaler. Group listings of authorities can be obtained providing information such as a list of boats permitted to operate in a particular fishery or details of all commercial fishers residing in a specific location.

Officers may find it necessary in the course of an investigation to request such information from Queensland Fisheries and are to obtain the authorisation of the OIC prior to making a request for information.

Officers requiring information are to complete a Form FDU1475: 'Application to inspect register of authorities' which is available from the Queensland Boating and Fisheries Patrol, DAF offices.

The OIC authorising the request should make the application on behalf of the Service and should complete the details and declaration on the Form FDU1475, acting on advice from the officer requiring the information. The reason for the request of information should be included in the 'Applicant Declaration' section of the form.

The Form FDU1475 should be lodged, with the applicable fee, at Queensland Fisheries who should be contacted prior to lodging the application for an estimate of fees.

7.1.4 Requesting information from Queensland Health

Section 142: 'Confidential information must not be disclosed' of the *Hospital and Health Boards Act* (HHBA) prohibits the disclosure by a designated person of any confidential information acquired if a person who is receiving, or has received a public sector health service could be identified from the information. However, a number of sections of the HHBA allow for the disclosure of confidential information in certain circumstances.

Definitions

For the purposes of this section:

Confidential information

see s. 139: 'Definitions for Part 7' of the HHBA.

Designated person

see s. 139: 'Definitions for Part 7' of the HHBA.

General medical condition

means the medical condition of a patient in general or non-specific terms, e.g. the patient's condition is 'satisfactory'.

Health professional

see Schedule 2: 'Dictionary' of the HHBA.

Health service

see s. 15: 'Meaning of health service' of the HHBA.

Health service facility

means Queensland Health or a hospital and health service facility.

Local police liaison officer

means a police officer designated as a point of contact between the relevant hospital and health service and the corresponding policing area.

Personal information

see s. 12: 'Meaning of personal information' of the *Information Privacy Act* (IPA).

Queensland Health staff member

means a 'designated person'

see s. 139: 'Definitions for Part 7' of the HHBA.

Disclosure under an agreement

The Service has a Memorandum of Understanding (MOU) with Queensland Health (QH) pursuant to s. 151(1)(b): 'Disclosure to Commonwealth, another State or Commonwealth or State entity' of the HHBA in relation to information exchange.

The MOU sets out the circumstances in which QH staff can disclose confidential or personal information to officers for the purposes of an investigation:

(i) of suspected criminal conduct engaged in by patients at health service facilities; or

(ii) to locate a patient who has been reported as a missing person.

Under the MOU, officers may request QH staff to disclose confidential or personal information which QH staff have acquired while acting in the course of their duties related to:

(i) a patient who has been reported as a missing person; or

(ii) suspected criminal conduct, or where QH staff are asked to provide written statements to assist officers to investigate and prosecute criminal offenders.

In addition, if an officer provides the name of the patient or a sufficient description to enable QH staff to identify the patient, the MOU authorises QH staff to confirm if the patient attended the health service facility and to disclose the patient's:

(i) name (if not known by the officer);

(ii) contact details; and

(iii) if relevant, their general medical condition,

regardless of where the:

(i) missing person was last seen; or

(ii) criminal conduct occurred.

Any disclosure by QH staff is subject to the requirement the staff member honestly and reasonably believes:

(i) a patient is a missing person; or

(ii) criminal conduct has been engaged in,

and they acquired the information whilst acting in the course of their duties. The MOU and IPA require QH staff to be satisfied on reasonable grounds the disclosure of any confidential or personal information is necessary for a law enforcement purpose.

The MOU does not interfere with existing lawful processes or legislative provisions which allow or require the acquiring or reporting of otherwise confidential information.

Officers who receive or investigate a complaint or report of an offence or suspected offence committed by a patient may request information (e.g. patient's name, contact details and, if relevant, the patients general medical condition) or a statement (i.e. statement of a witness or victim) from QH staff to assist in the investigation and/or prosecution of the offender.

Officers who are attempting to locate a person who has been reported as missing, may request information (e.g. patient's name, contact details and, if relevant, the patient's general medical condition) or a statement (i.e. statement of a witness) from QH staff to assist in locating the missing person.

Officers making a verbal or written request for information or a statement from QH are to, as far as practicable, provide:

(i) brief particulars of the offence or incident being reported or investigated including the date, time and location;

(ii) the name, date of birth or description of the:

(a) patient reported as a missing person;

(b) patient suspected of committing the offence; or

(c) QH staff from whom the information or statement is required;

(iii) the type and nature of information required;

(iv) the reasons why the information is required and the purpose for which it will be used;

(v) the name, rank, station/establishment, and contact details of the requesting officer; and

(vi) if the disclosure of the confidential information is being sought by consent, officers should include a copy of the signed QP 0886: 'Consent to disclosure of confidential information to police' (see the subsection titled 'Disclosure with consent' of this section).

In making requests, officers are to comply with any local protocols between the relevant policing area and health and hospital service to give effect to the MOU.

Officers are to note that QH staff may, due to confidentiality, privacy or other legitimate concerns, seek independent legal advice in relation to any Service requests for confidential or personal information and are entitled to refuse to voluntarily cooperate with such requests. However, QH staff are encouraged by QH to cooperate with Service requests for information where they are relevant and such information ought to be disclosed.

Where prescribed circumstances exist, officers may require QH staff to provide their correct name and address pursuant to s. 40: 'Person may be required to state name and address' of the PPRA however, voluntary cooperation should always be sought first before making a requirement.

Urgent requests for information

Officers requiring information (e.g. witness or patient's name and contact details) in circumstances where an immediate response is required to ensure the safety of any person or apprehension of an offender, should make a verbal request direct to relevant QH staff or emergency department or other area within QH responsible for releasing the information.

Where practicable, verbal requests are to be made in person. QH staff are likely to refuse requests for information over the telephone unless it can be clearly established the person to whom they are speaking to is a police officer.

Non-urgent requests for information

When non-urgent information or a statement is required from QH staff for an investigation or prosecution, the investigating officer is to make a written request to the relevant QH facility or area within QH responsible for releasing the information. Where applicable, these requests should be made through the local police liaison officer.

All requests for non-urgent information or statements should be by:

(i) QP 0887: 'Police request for access to confidential information held by Queensland Health';

(ii) letter on Service letterhead; or

(iii) external Service email,

addressed to the Health Information Manager or Release of Information Officer in the relevant health and hospital service. The written request may be delivered by facsimile, email, post or in person.

Accessing medical records and other confidential documents

Officers requiring access to, or copies of, a patient medical record or part of an employee's personnel file should, where practicable, obtain the consent of the patient or employee to access the record or file. Officers should use a QP 0886 for this purpose.

If consent is not forthcoming, or the original record or document is required as evidence, officers should use other appropriate lawful means in obtaining the information such as a search warrant, summons to witness or subpoena.

Disclosure required or permitted by law

Section 142: Confidential information must not be disclosed' of the HHBA allows the disclosure of confidential information by a designated person if the disclosure is required or permitted by an Act or another law. In addition to search warrants, subpoenas and summons of a witness, several avenues exist for the obtaining of information or documents under s. 142 of the Act including:

(i) coronial matters:

Under s. 597: 'Powers for reportable deaths' of the PPRA, an officer may seize anything at the place of a reportable death the officer reasonable suspects may be relevant to an investigation of the death by a coroner. The relevant medical records of the deceased patient may be seized to assist in the investigation where a death occurs in a health facility (see s. 8.5.3: 'Health care related deaths' of the OPM). See also s. 2.8.6: 'Coroner's search warrant' of the OPM.

Under s. 601: 'Power to require information' of the PPRA an officer helping a coroner to investigate a death may require a person to give information relevant to the investigation of the death. When making the requirement, the officer must inform the person that the person may fail to give information if the information would tend to incriminate the person, and to seek legal advice before giving the information.

Under s. 16: 'Duty to help investigation' of the *Coroners Act*, a coroner may issue a Form 25: 'Requirement by coroner for information' to require a person to give information relevant to the investigation of the death. When making the requirement, the officer must inform the person that the person may fail to give information if the information would tend to incriminate the person, and to seek legal advice before giving the information.

Section 157: 'Disclosure to person performing functions under Coroners Act 2003' of the HHBA also allows the disclosure of confidential information to a person who requires the confidential information to perform a function under the *Coroners Act*. See the subsection titled 'Accessing Queensland Health information' of this section. See also Chapter 8: 'Coronial matters' of the OPM;

(ii) children:

Section 144(d): Disclosure with consent' of the HHBA allows a designated person who is a health professional to disclose confidential information where the person is a child and the health professional reasonably believes the disclosure is in the child's best interest. Such a situation may exist in child abuse cases.

Additionally s. 159O: 'Release of information by a health services designated person' of the *Child Protection Act* allows a designated person under the HHBA to give a police officer confidential information where it is relevant for the protection or wellbeing of a child. See also Chapter 7: 'Child Protection' of the OPM; and

(iii) provisions of the *Prostitution Act*:

Health professionals, as defined in s. 134A: 'Protection of health professionals from liability' of the *Prostitution Act*, may provide an officer with information about a prostitute at a licensed brothel where the health professional reasonably believes that the prostitute is a person with an impairment of the mind.

Disclosure with consent

The disclosure of confidential information by QH staff is permitted under s. 144: 'Disclosure with consent' of the HHBA if the person to whom the confidential information relates is:

(i) an adult and consents to the disclosure (see s. 144(a) of the HHBA); or

(ii) a child and the disclosure of the confidential information is by a health professional who reasonably believes:

(a) the child is of sufficient age and mental and emotional maturity to understand the nature of consenting to the disclosure, and the child consents to the disclosure (see s. 144(b) of the HHBA);

(b) the child is of insufficient age or mental or emotional maturity to understand the nature of consenting to the disclosure, and the child's parent or guardian consents to the disclosure (see s. 144(c) of the HHBA); or

(c) the disclosure of the information is in the child's best interests (see s. 144(d) of the HHBA).

Officers requiring confidential information in patient medical records or personnel files in circumstances not covered by the MOU, should where practicable, request the written consent of the person for that information.

Officers should:

(i) request the person sign a QP 0886; and

(ii) scan the completed QP 0886 into the relevant QPRIME occurrence and attach the original document to the QP 0758: 'Occurrence report' or investigation file.

Once written consent is obtained, officers should comply with the subsection titled 'Non-urgent requests for information' of this section.

If consent is revoked prior to obtaining the confidential information, officers are not to use the revoked written consent form. The date of revocation should be clearly noted on the form and within the QPRIME occurrence. The 'remarks' tab of the scanned document in QPRIME is to be amended to indicate consent has been revoked.

Medicines Regulation and Quality Team, Health Protection Unit

Documents which may be available from the Medicines Regulation and Quality Team, Health Protection Unit, QH (MRQT) include:

(i) duplicate copies of prescriptions for controlled drugs dispensed in Queensland during the previous two years;

(ii) information pertaining to a specified person about treatment with a controlled drug; and

(iii) summary data of all controlled drugs obtained by a specified person over the preceding two year period.

In all cases where documents are sought from the MRQT for the purpose of an investigation (unless the investigation relates to staff at the unit or an associate of staff) should:

(i) contact them (see SMCD) to discuss the nature of the document sought and determine whether it is held by the Drugs of Dependence Unit;

(ii) obtain a description of the document suitable for inclusion on a search warrant;

(iii) determine a time suitable to both the officer and the MRQT at which to execute a search warrant; and

(iv) obtain a search warrant which specifies the documents to be seized and is valid for the time previously determined as most suitable for the execution of the search warrant (see s. 2.8.3: 'Obtaining a search warrant' of the OPM).

Particular care must be taken when disclosing information received from the MRQT as in some cases its disclosure may reasonably be expected to prejudice the effectiveness of a lawful method or procedure for preventing, detecting, investigating or dealing with a contravention or possible contravention of the law (see s. 803: 'Protection of methodologies' of the PPRA).

Information received from the MRQT, other than documents which are to be tendered to a court as evidence, is not to be disclosed to any external agency or person except as required by law.

When information or material received from the MRQT is required to be disclosed in an impending court proceeding, the police prosecutor responsible for the prosecution is to notify the Manager, MRQT at least 14 days before the commencement of the relevant proceeding for the purpose of ascertaining whether any grounds exist to object to the disclosure of the information or material under s. 590AQ: 'Limit on disclosure contrary to the public interest' of the Criminal Code on the basis that the disclosure would be contrary to the public interest. Such notification will allow any subsequent claim under s. 590AQ of the Criminal Code regarding the documents disclosed by the MRQT to be made by the prosecution.

The notification is to be provided to the Manager, MRQT by letter on Service letterhead, including:

(i) the name and date of birth of the person;

(ii) the relevant court;

(iii) brief particulars of the offence; and

(iv) the date of the relevant proceeding.

The letter may be sent to the Manager, MRQT by email (see SMCD).

Police prosecutors are to ensure copies of such letters, associated facsimile transmission reports, emails and subsequent replies are attached to the prosecutions copy of the Court Brief (QP9).

If a member is questioned about such information during a proceeding, prosecutors are to bring the provisions of s. 803: 'Protection of methodologies' of the PPRA to the notice of the court. Members are not to disclose information obtained from the MRQT to a court unless directed to do so by the court.

Queensland Health seeking investigative information from the Service

Members receiving requests for investigational information from QH in relation to QH staff, facilities or property not otherwise provided in accordance with the *Victims of Crime Assistance Act* (see s. 2.12: 'Victims of crime' of the OPM) should refer s. 5.6.14: 'Requests for information from other government department, agencies or instrumentalities' of this Manual).

Restrictions on obtaining or using COVID-19 application information

Chapter 8, Part 7A, Division 6: 'Protection of personal information' of the *Public Health Act* sets out how COVID-19 application information can be used and when it can be disclosed. In accordance with the division, the information can only be used for the purposes as defined in the Act and cannot be obtained by use of court orders or search warrants.

7.1.5 Transport registration and integrated licensing system information suppression

The Department of Transport and Main Roads maintains the Transport Registration and Integrated Licensing System (TRAILS). The TRAILS database contains personal particulars and address details as Queensland Transport customer records. This database is accessible by employees of a number of Government agencies as well as authorised persons within the community such as some legal practitioners and insurance company employees. While access to personal information is controlled there is still a risk that personal information may be accessed in circumstances that create a threat to a person's personal safety.

In order to minimise this risk, the Department of Transport and Main Roads allows agencies such as the Queensland Police Service and individuals to apply to have access to particular Queensland Transport customer records suppressed in certain circumstances.

Suppression of a Queensland Transport customer record has the effect of making that record unavailable to users of TRAILS, including members of the Service.

Queensland Transport customer record suppression applications

Officers are generally only to initiate or support applications in cases where:

(i) it is reasonably suspected that significant harm to the subject person is likely if their personal details became known to a particular person or group of people (the **'threat'**); and

(ii) the threat has or may have access to the person's Queensland Transport customer record; or

(iii) the threat has previously discovered or attempted to discover the address or personal particulars of the subject person or persons in a similar situation.

In cases that do not meet the criteria to justify an officer initiating or supporting an application, officers are to advise the person to complete a Form F4109: 'Customer Record Suppression Application' as a private individual, attach a copy of the relevant court order and send the application to the Department of Transport and Main Roads.

Applications to suppress access to a member's Queensland Transport customer record may be made where there are particular circumstances that indicate that the member's safety is, or may be, at risk, such as the member being subject to threats or for some other good reason.

Officers who believe that it is necessary to apply, or support an application, for the suppression of access to a person's Queensland Transport customer record, to reduce a risk to a person's or persons' safety should:

(i) prepare a report detailing:

(a) the name, address and date of birth of each person whose details are to be suppressed;

(b) the reasons why the person's details are to be suppressed;

(c) whether it is necessary to restrict or permit access to the Queensland Transport customer record by any member of the Service. The reasons why access should be denied, or given, to any particular member are to be fully detailed; and

(d) the period for which access to the person's Queensland Transport customer record should be suppressed;

(ii) assist each person for whom access suppression is sought to complete a Form F4109: 'Customer Record Suppression Application' (available from the Department of Transport and Main Roads Docbase3 web page or from a Department of Transport and Main Roads Customer Service Centre).

(iii) attach a copy of any relevant court order; and

(iv) submit the completed documents to their supervising commissioned officer.

Commissioned officers receiving applications for the suppression of Queensland Transport customer records should consider whether:

(i) there is a significant risk to the safety of a person;

(ii) the suppression of access to the person's record would reduce that risk; and

(iii) there is a need to restrict access by particular members of the Service where a request of this nature is made, bearing in mind that denying access to all but a few members of the Service to access suppressed records can significantly hamper effective operations.

Where a commissioned officer considers that it would be appropriate to suppress access to a person's Queensland Transport customer record, the commissioned officer should:

(i) prepare written advice to the Department of Transport and Main Roads giving:

(a) a firm recommendation that the record should be suppressed;

(b) the period of such suppression; and

(c) the name of any members who should not be permitted access to the record or alternatively the names of those members who should be permitted access to the record;

(ii) forward the file to the Department of Transport and Main Roads.

Where a commissioned officer considers that it is not necessary to suppress access to a person's Queensland Transport customer record, the commissioned officer should advise the member who prepared the originating report. The member who prepared the originating report should advise the person to whom the report related that the Service does not support the application but the person may apply to Queensland Transport for the suppression of their Queensland Transport customer record as a private individual.

A commissioned officer who receives an application which requests that a particular member of the Service not be permitted access to a suppressed Queensland Transport customer record is to forward a copy of the file to the State Coordinator, Internal Investigations Branch, Ethical Standards Command for information.

Accessing suppressed Queensland Transport customer records

Suppressed Queensland Transport Customer Records are indicated by the response 'Refer to QT Security Officer' when the record is queried through TRAILS or QPRIME. In such cases access to the relevant Queensland Transport customer record may only be obtained from the Identity Management Unit, Queensland Transport during normal business hours.

Members who require access to a suppressed Queensland Transport Customer Record are to:

(i) prepare a brief report stating:

(a) the name and date of birth (if known) of the relevant person or the registration number of the relevant vehicle or vessel;

(b) the nature of the information sought from the suppressed Queensland Transport customer record, e.g. driver licence particulars, registration particulars or other licence particulars;

(c) the reason why the information is necessary for the performance of the member's duty, e.g. for an investigation or to establish a person's current address to execute a warrant;

(d) contact details for the inquiring officer including a facsimile number or email address for the requested information to be forwarded to; and

(ii) forward the report to their supervising commissioned officer for approval.

Commissioned officers who receive such reports are to determine whether access to the record is necessary for the performance of the member's duty. If access to the record is considered to be necessary, the commissioned officer is to endorse the report and forward it to the Identity Management Unit, the Department of Transport and Main Roads by email (see SMCD).

The Identity Management Unit, the Department of Transport and Main Roads will forward the required information directly to the inquiring member unless the member is not permitted to access the suppressed Queensland Transport customer record. In such cases the Identity Management Unit will advise the commissioned officer who endorsed the original 'Customer Record Suppression Application' to determine the most appropriate course of action.

Commissioned officers who are advised that a member has sought access to a suppressed Queensland Transport customer record to which the member is specifically denied access (i.e. named in the original 'Customer Record Suppression Application'), are to report the matter to the State Coordinator, Internal Investigations, Ethical Standards Command.

7.1.6 Requesting information from Workplace Health and Safety Queensland or the Electrical Safety Office (Office of Industrial Relations)

Workplace Health and Safety Queensland

The Office of Industrial Relations administers the workplace health and safety program through Workplace Health and Safety Queensland. The responsibilities of the unit are to:

(i) provide information and education;

(ii) maintain a workplace health and safety regulatory framework that meets the needs of industry and government; and

(iii) ensure compliance within the regulatory framework.

The *Work Health and Safety Act* is enforced by inspectors from Workplace Health and Safety Queensland. Inspectors are appointed under the *Work Health and Safety Act*, and are based in offices throughout Queensland (see SMCD) and visit workplaces in all sectors of industry.

Primarily the role of an inspector involves monitoring and ensuring compliance with workplace health and safety legislation. It is also the role of an inspector to provide information and ensure obligation holders comply with their legislative requirements.

Inspectors visit workplaces for a variety of reasons including to:

(i) investigate workplace incidents;

(ii) investigate reports of unsafe or unhealthy conditions and dangerous work practices;

(iii) assess workplace health and safety risks to workers and members of the public;

(iv) conduct workplace health and safety audits; and

(v) provide information and advice on the legislation.

Electrical Safety Office

The Office of Industrial Relations, Electrical Safety Office is responsible for developing and enforcing standards for electrical safety and promoting strategies for improved electrical safety performance across the community.

The Electrical Safety Office facilitates socially responsible and safe electrical industry practices by:

(i) developing and implementing electrical safety legislation, standards and initiatives;

(ii) enforcing the electrical safety legislation;

(iii) investigating electrical incidents, complaints and unlicensed and unsafe electrical work;

(iv) approval and registration of electrical equipment;

(v) administering a licensing regime;

(vi) providing information products, education and advisory services; and

(vii) promoting the safe use of electricity within the community.

The *Electrical Safety Act* establishes the legislative framework for electrical safety in Queensland and is supported by the Electrical Safety Regulation and three Codes of Practice.

The *Electrical Safety Act* is enforced by inspectors from the Electrical Safety Office. Inspectors are appointed under the Act, and are based in offices throughout Queensland (see SMCD).

Primarily the role of an inspector involves monitoring and ensuring compliance with electrical safety legislation. It is also the role of an inspector to provide information and ensure obligation holders comply with their legislative requirements.

Requesting information from Workplace Health and Safety Queensland or Electrical Safety Office

In the course of an investigation of a workplace or electrical incident, officers may find it necessary to request information from Workplace Health and Safety Queensland or the Electrical Safety Office. Material relating to an investigation that may be requested includes:

(i) witness' statements;

(ii) photographs of the scene;

(iii) sketches and notes made at/of the scene;

(iv) workplace health and safety inspectors' statements;

(v) electrical inspectors' statements;

(vi) measurements and other tests/examinations performed;

(vii) documents obtained that are required to be kept under the *Work Health and Safety Act* or *Electrical Safety Act*;

(viii) any other facts relating to the incident;

(ix) legal, statutory or other privileged documents, e.g. expert reports;

(x) commercially sensitive material, e.g. tender documents, project specifications, contracts and safety plans;

(xi) documents that have been received from another department or agency; and

(xii) documents that contain statements provided 'In confidence', e.g. where a person wants their confidentiality to be maintained.

Officers requesting information from Workplace Health and Safety Queensland or the Electrical Safety Office are to:

(i) complete QP 0658: 'Request Information From WPH&S Or ESO';

(ii) obtain authorisation from the officer in charge of their station or establishment;

(iii) transmit the request:

(a) for material that includes documents (i) to (viii) of the list above, to the appropriate Workplace Health and Safety Queensland or Electrical Safety Office (see SMCD); or

(b) for material that includes documents (ix) to (xii) of the list above, to the Regional Investigation Manager, Regional Services Branch, Workplace Health and Safety Queensland (see SMCD).

For further information in relation to workplace or electrical incidents, their investigation and the sharing of information, see s. 2.6.11: 'Workplace and electrical incidents' of the Operational Procedures Manual.

7.1.7 Requesting information from Registry of Births, Deaths and Marriages

Members requiring searches relating to Births, Deaths, Marriages and Change of Name Certificates for an investigation are to ensure all Service intelligence holdings have been thoroughly checked prior to making any formal requests.

Certificates signed by the Registrar will not be provided free of charge unless requested for court purposes.

Certificates signed by the Registrar will only be sent via Australia Post. Members are to be mindful of postage timeframes when making requests. In exceptional circumstances the Registry will consider scanning and emailing a certificate where the certificate is password protected. These requests will be assessed on a case-by-case basis and is at the discretion of the Registrar.

Members requesting information or certificates from Registry of Births, Deaths and Marriages are to complete a written request on Service letterhead and forward via email. (see SMCD).

Members are to outline in this request the following:

(i) if known, name, date of birth and place of birth;

(ii) the upcoming court date and location; and

(iii) if the requesting member requires an original document or whether a name search will suffice.

Members requesting information from an interstate births, deaths and marriages office are to complete an 'External Agency Request' available on the State Intelligence Group, Crime and Intelligence Command webpage of the Service Intranet.

Urgent requests for information

Members requiring urgent searches related to births, deaths and marriages are to complete a written request as outlined above and must include 'urgent' in the subject line. Members should clearly establish the need for an urgent response in the request. Urgent requests will usually be responded to within 24 hours of receipt. In circumstances where requests are received after 3pm, a same day response in not guaranteed by the Registry.

7.1.8 Requesting information from Department of Resources

Before requesting a search from the Department of Resources, officers are to ensure that Service intelligence holdings have been thoroughly checked.

Where an officer requires a search of ownership of land, and/or properties, a written request is to be forwarded to Titles Queensland, info@titlesqld.com.au (see SMCD). The request is to include:

(i) name of owner;

(ii) date of birth of owner; and

(iii) property or land numbers, including registered plan number if known.

7.1.9 Requesting information from the Department of Education

Requests for information held by the Department of Education may be released:

(i) with written consent of the Chief Executive or delegate when:

(a) there is a 'serious risk to the life, health or safety of a person';

(b) it is in the 'public interest'; or

(c) the 'information is necessary for the prevention, detection, investigation, prosecution or punishment of a criminal offence or a breach of a law imposing a penalty or sanction',

(see s. 426(4)(e): 'Confidentiality' of the *Education (General Provisions) Act* (E(GP)A)).

Officers requesting information should complete a:

(d) LEA 1: 'Request from a law enforcement agency (LEA) to release student personal information to assist in averting a serious risk to the life, health or safety of a person OR where the disclosure is in the public interest'; or

(e) LEA 2: 'Request from an LEA to release personal information for the prevention, detection, investigation, prosecution or punishment of a criminal offence',

(link also on Form Select) and forward the signed request form to the relevant delegate of the Chief Executive:

(f) in the first instance, request it from the school principal where the information is believed to be held, or

(g) if the school principal is unavailable, or unable to provide the requested information, the regional director may be contacted,

(see SMCD). Principals and regional directors can only exercise the power where the information concerns a student who attends a school within the area of their administrative responsibility;

(ii) with the consent of the person to whom the information relates or for a child unable to consent, the consent of a parent (see s. 426(4)(b) of the E(GP)A). Consent to obtain information should be recorded in an official police notebook; or

(iii) as permitted or required by another Act (see ss. 426(4)(d) of the E(GP)A and 7.9.1: 'Relevant information exchange' and 2.8.3: 'Obtaining a search warrant' of the OPM).

The Department of Education's document 'Disclosing personal information to law enforcement agencies' provides further information is available from their Policy and Procedures Register internet site.

7.1.10 Requesting information from the Department of Transport and Main Roads

Members requiring information relating to the Department of Transport and Main Roads are to ensure that all Service information/intelligence holdings have been exhausted before any request is made.

Where the required information is not available on all Service holdings (e.g. historical vehicle information, information pertaining to 18+ cards, certificates for court purposes) members may request the information from the Department of Transport and Main Roads.

When requesting information from the Department of Transport and Main Roads, members are to first consider requesting the information under a legislative scheme that may authorise the release of the information. Where no legislative scheme exists which authorises the release of information, members may request the information be released under the *Information Privacy Act*.

Requests for certificates for court production are to be submitted in compliance with the subsection 'Requests for information under a legislative scheme'. Due to the volume of applications received by the Department of Transport and Main Roads, officers should make application for a certificate at least three weeks before the court date.

Requests for information under a legislative scheme

Where the information required falls under a legislative scheme enabling the Department of Transport and Main Roads to release information, the request for information is to be made on Service letterhead. Information the Department of Transport and Main Roads may provide under a legislative scheme includes:

(i) a person's current and/or historical licence details or accreditation under s. 77: 'Restricted written release of person's prescribed authority and traffic history information' of the *Transport Operations (Road Use Management) Act*;

(ii) a person's marine licence details or marine history under s. 63I: 'Restricted written release of information' of the *Transport Operations (Marine Safety) Act*;

(iii) a person's driver authorisation to provide a public passenger service under s. 35H: 'Restricted written release of information' of the *Transport Operations (Passenger Transport) Act*;

(iv) a person's 18+ card under s. 30: 'Restricted release of information in APA register' of the *Photo Identification Card Act*;

(v) whether a licence is a valid or fraudulent licence under s. 77: 'Restricted written release of person's prescribed authority and traffic history information' of the *Transport Operations (Road Use Management) Act*; and

(vi) current and/or historical vehicle registration details under s. 202: 'Giving extracts from register to eligible persons' of the Transport Operations (Road Use Management–Vehicle Registration) Regulation.

Members requesting the release of information or the issuing of a certificate for court from the Department of Transport and Main Roads under a legislative scheme are to request the information in writing on Service letterhead including:

(i) the person's name and Customer Reference Number/driver licence number;

(ii) the date of the offence (if known);

(iii) the QPRIME occurrence number;

(iv) the date the brief of evidence is due (if known);

(v) information that is required;

(vi) reason for requesting the information;

(vii) section and Act that authorises the release of the requested information (if known);

(viii) requesting officers details; and

(ix) how the information or certificate is to be delivered to the officer (e.g. collect in person or facsimile).

Requests for information or the issuing of a certificate for court are to be submitted to the Department of Transport and Main Roads through the investigating officer's local Department of Transport and Main Roads Customer Service Centre.

Urgent requests for information under a legislative scheme

Officers requiring information in circumstances where an immediate response is required to ensure the safety of any person or apprehension of an offender, may make a verbal request in person at a Department of Transport and Main Roads Customer Service Centre after producing their official police identification. Where the Department of Transport and Main Roads Customer Service Centres have access to the requested information, they may provide the results of the search verbally.

Where the information request is required to be forwarded to another unit within the Department of Transport and Main Roads for processing, members are to request the information in writing on Service letterhead.

Officers are to note that the Department of Transport and Main Roads staff members may, due to privacy or other legitimate concerns, seek advice in relation to any verbal requests for information and are entitled to refuse such requests.

Requests for information under the Information Privacy Act

Where the information required does not fall under one of the legislative schemes for the Department of Transport and Main Roads to release information (e.g. for intelligence purposes such as requesting details of when a person has attended a the Department of Transport and Main Roads Customer Service Centre, or establishing how a fee was paid), members may request the information from the Department of Transport and Main Roads, who can consider releasing the information under Schedule 3, Information Privacy Principle 11 of the *Information Privacy Act*.

Members requesting information from the Department of Transport and Main Roads to be considered for release under Schedule 3, Information Privacy Principle 11 of the *Information Privacy Act* are to:

(i) complete a QP 0904: 'DTMR – Request for Law Enforcement Information Under the Information Privacy Act';

(ii) obtain authorisation of a supervising officer to make the request; and

(iii) forward the completed form to the Department of Transport and Main Roads Customer Service Centre.

The Department of Transport and Main Roads will forward the results directly to the requesting officer.

7.1.11 Accessing digital photos from the Department of Transport and Main Roads

The Department of Transport and Main Roads (DTMR) captures and stores digital photos of persons applying for a Queensland driver licence.

Authority to access Department of Transport and Main Roads digital photo database

Section 28ED(4): 'Restricted access to a digital photo and digitised signature' of the *Transport Planning and Coordination Act* (TPCA) provides the authority for DTMR to share driver licence images with the Service for transport and non-transport law enforcement purposes (see Criminal Law Bulletin No. 315: 'Use of TMR photos for Police Investigations etc.').

Accessed images must be for a permitted purpose

An officer accessing DTMR digital photos under s. 28EP: 'Disclosure, use or collection must be for permitted purpose' of the TPCA are to only to do so for a permitted purpose.

Access to DTMR database

Access to DTMR digital photos database can be made using a QLiTE device or if an officer does not have access to a QLiTE device, the officer may email a request directly to the DTMR Identity Management Unit.

Obtaining digital photos from the Department of Transport and Main Roads

Where an officer considers obtaining a digital photo from DTMR is necessary for a reason described in s. 28EP of the TPCA, the officer is to:

(i) exhaust all available Service databases for a suitable image of the person (e.g. QPRIME);

(ii) conduct a Queensland driver licence check of the person on a QLiTE device. Where the text "TMR Image Available" is displayed, a digital photo is held by the DTMR. Obtain the person's DTMR Customer Reference Number (CRN) (**'Licence number'**).

Where an officer does not have access to a QLiTE device, the officer should:

(a) conduct a QPRIME Queensland driver licence check of the person to obtain the person's DTMR CRN (**'Licence number'**); and

(b) telephone the DTMR Identity Management Unit (see SMCD) to confirm a digital photo of the person is available; and

(iii) email an image release request to the DTMR Identity Management Unit (see SMCD) clearly stating the purpose of its usage (see s. 28EP of the TPCA).

Officers making an email request for a digital photo for use in a photo board should request a jpeg version and watermark removed from the photo.

Storage and dissemination of a digital photos

Officers are to take all reasonable precautions to ensure a digital photo is not copied or disseminated beyond the permitted purpose (see s. 28EP of the TPCA) for which it was accessed or released.

Where a copy of the digital photo is provided to another officer, the officer providing the image is to maintain a record of the dissemination in the relevant QPRIME 'Occurrence inquiry log'.

Digital photos obtained from DTMR are to be:

(i) deleted if no longer required; or

(ii) stored in accordance with subsection 'Retention of non-evidential digital photographs' of s. 2.5.5: 'Use of digital still cameras' of the OPM; and

(iii) not uploaded into QPRIME unless operationally necessary.

7.2 Federal departments

7.2.1 Australian Taxation Office

For the purpose of this section:

Authorised law enforcement agency officer

means a senior officer of the Service authorised in writing by the Commissioner (see Delegation D 119.1).

State Intelligence Group, Crime and Intelligence Command will provide a list of authorised law enforcement agency officers to the Australian Taxation Office (ATO), which is also available on the State Intelligence Group, Crime and Intelligence Command webpage on the Service Intranet. The ATO will only process requests received from the list of authorised law enforcement agency officers provided.

Information held by the ATO may, under certain circumstances (see s. 355-70: 'Exception–disclosure for law enforcement and related purposes' located in Schedule 1, Chapter 5: 'Administration' of the *Taxation Administration Act* (Cwlth) (TAA)) be requested by officers performing the functions of an authorised law enforcement agency officer. Any information received under s. 355-70 is subject to audit by the Queensland Privacy Commissioner to ensure the use of the information obtained has been limited to the defined purposes set out in that section.

Requests for information from the ATO are only to be made when the information requested cannot be obtained from other sources. Officers performing the functions of an authorised law enforcement agency officer may apply, under s. 355-70 of the TAA, to the Commissioner of Taxation for the release of information for the purpose of:

(i) investigating an offence punishable by more than 12 months imprisonment;

(ii) enforcing the law, the contravention of which is punishable by more than 12 months imprisonment; or

(iii) the making, or proposed possible making, of a proceeds of crime order.

Requesting information

Officers who reasonably believe that information essential to that investigation is only available from ATO records should:

(i) complete the 'ATO Information Disclosure Request Form' available via the State Intelligence Group webpage on the Service intranet; and

(ii) forward the Information Disclosure Request Form to the relevant authorised law enforcement agency officer.

ORDER

A request made to an authorised law enforcement agency officer is to specify the following:

(i) the names, last known addresses and other relevant details of the persons under suspicion and their associates;

(ii) the nature of the offence(s) being investigated;

(iii) the statute and section which provides the offence being investigated is indictable, or under which a proceeds of crime order may be made;

(iv) the penalty prescribed for the offence; and

(v) the precise nature of the information sought, the reason it is required and its relevance to the investigation.

Officers are not to voluntarily disclose information supplied under s. 355-70 of the TAA as evidence in a court except in the case of tax related prosecutions or post-conviction proceeds of crime order proceedings.

Officers are not to divulge to any person or make a record of any information received subject to a request under s. 355-70 of the TAA except for the purpose of or in connection with the original purpose the information was sought.

Processing requests for information

Authorised law enforcement agency officers are to examine each request they receive for information held by the ATO to determine whether the request is one which can be appropriately made under s. 355-70 of the TAA.

An authorised law enforcement agency officer, who is satisfied that the taxation information request is appropriate is to process the Information Disclosure Request Form which will generate an email to the ATO.

Record keeping

The ATO will disseminate responses to requests to the Intelligence Support Team, State Intelligence Group, Crime and Intelligence Command who will disseminate them to the requesting officer.

ORDER

Members who receive information under s. 355-70 of the TAA are to ensure they:

(i) comply with ss. 355-155 and 355-175 of the TAA; and

(ii) make a record of any recording or further disclosure of the information.

The use and disclosure of the information is reviewable by the Queensland Privacy Commissioner.

7.2.2 ACC database (system for the national exchange of police information)

The ACC database contains various components, several of which are accessible to operational officers.

National Police Reference System

The ACC has established a database called the National Police Reference System.

The National Police Reference System contains records drawn from the Persons of Interest systems of all Australian police services and are available through QPRIME.

The National Police Reference System provides personal information including:

(i) names including aliases;

(ii) addresses;

(iii) if the person is wanted on warrants, orders or subject to court notices;

(iv) if the person is subject to a domestic violence restraining orders;

(v) criminal history

(vi) being charged with an offence;

(vii) being reported as a missing person;

(viii) weapons license details including if the person has an adverse weapons history;

(ix) being wanted for questioning for an offence;

(x) cautions and warnings;

(xi) fingerprint details, CNI and driver licence details;

(xii) physical descriptions, photographs, tattoos and other distinguishing marks or features;

(xiii) if the person is a current or previous escapee; and/or

(xiv) details relating to bail and parole.

If a check on the National Police Reference System reveals a person is wanted for questioning or on warrant, is a missing person or has criminal history and this information is not sufficient for the required purpose, the officer initiating the check may forward a request to the Manager, Police Information Centre, to enable full details to be obtained.

An audit log is kept of all transactions on the National Police Reference System.

Officers making National Police Reference System checks are to comply with the instructions contained in QPRIME User Guide.

The Manager, Police Information Centre is to ensure that requesting officers are advised of the outcome of requests. Where information requested has been obtained, the Manager, Police Information Centre is to forward the information to the requesting officer in a manner that maintains an appropriate level of confidentiality and security.

Officers forwarding requests in accordance with the above policy should include details of:

(i) the reason the information is required;

(ii) the file reference number (docket number) of the subject person; and

(iii) the name, rank, registered number and station, establishment or section of the officer making the request.

Officers may forward requests by QPRIME task to Release Unit Police (ORG Unit 3272).

ORDER

Members are not to produce screen prints of National Police Reference System information to courts or to any external organisation.

Access to ACC database

Officers requiring access to ACC database are to:

(i) complete a QP 0410: 'Application for Computer Access – ACC Database';

(ii) have the QP 0410 endorsed by their officer in charge of the requesting officer; and

(iii) forward the form via facsimile or mail to Frontline and Digital Division.

7.2.3 Services Australia (Centrelink, Medicare and Child Support)

Services Australia is responsible for administering the federal:

(i) Centrelink;

(ii) Medicare; and

(iii) Child Support,

agencies through a number of legislative arrangements.

Police officers, during the course of an investigation, may find it necessary to request information from Services Australia. Guidelines have been established in relation to requests for disclosure of information concerning clients of that department.

The *Privacy Act* (Cwlth) and the various Acts administered by Services Australia protect the personal information of clients from access by unauthorised persons.

However there are limits to this protection. Where it can be established that it is in the public interest to release personal information a release can be authorised:

(i) where the release of information is 'necessary'; and

(ii) after all Service information/intelligence sources have been exhausted.

In accordance with the relevant Commonwealth legislation, each agency has specific circumstances where information may be released to the Service.

Each request is to provide as much information as possible to support the release of the otherwise protected information and assist with identifying the individual. Unless an absolute match can be made information will not be released.

ORDER

All requests for information from Services Austraila are to be approved by a commissioned officer.

Requests for information from Centrelink

Information may be sought from Centrelink when the information cannot be obtained from another appropriate source and is 'necessary' in relation to:

(i) a criminal offence which must:

(a) be indictable with a term of imprisonment of two or more years; or

(b) have a pecuniary penalty of 40 penalty units; or

(c) have a significant adverse effect on public revenue;

(ii) an inquired person who is deceased;

(iii) an inquired person who is reported as missing, as per arrangements with the Missing Persons Unit, Crime and Intelligence Command; or

(iv) to prevent a threat to the life, welfare or health of a person.

Requests for information from Medicare

Information may be sought from Medicare in relation to the:

(i) Commonwealth Medical Benefits Scheme (Medicare); and

(ii) Pharmaceutical Benefits Scheme,

when the information is cannot be obtained from another appropriate source and is necessary to assist or support a police investigation in relation to:

(i) a major criminal investigation;

(ii) a threat to life, health and welfare of a person or to assist a health provider to contact a patient;

(iii) an inquired person who is deceased; or

(iv) an inquired person who is reported as missing, as per arrangements with the Missing Persons Unit, Crime and Intelligence Command.

ORDER

Officers who are provided with information from Medicare, are then responsible for this information and are subject to the same rights, privileges, obligations and liabilities as if they were an officer under s. 130(4) of the *Health Insurance Act* (Cwlth). The information provided remains subject to the *Health Insurance Act* (Cwlth) and shall not be divulged or communicated to any other person without the authority of the Federal Minister for Health.

Requests for information from Child Support

There is no authority to release information held by Child Support for a law enforcement purpose.

A request for information from Child Support may be made when the information cannot be obtained from another appropriate source and is necessary to support a police investigation in relation to:

(i) an imminent threat to the life, health or welfare, or evidence of such a threat being made, to an inquired person;

(ii) an inquired person who is deceased; or

(iii) an inquired person who is reported as missing, as per arrangements with the Missing Persons Unit, Crime and Intelligence Command.

ORDER

Any request for information from Child Support is to include as much detail as appropriate to assist the Department of Human Services in determining whether to release the requested information.

Processing requests for information

PROCEDURE

Officers seeking information from Services Australia are to:

(i) obtain commissioned officer approval through their chain of command; and

(ii) complete a QP 0973: 'Police request for confidential information held by Services Australia', ensuring the following information is included:

(a) whether the request is routine or urgent;

(b) that the disclosure requested is in the public interest;

(c) full name (including aliases) and date(s) of birth of the person(s) about whom the information is sought;

(d) the information requested and the reason for the request;

(e) for requests from Centrelink, certification that the information sought cannot reasonably be obtained from a source other than Centrelink, including Queensland Police Service sources and databases; and

(f) the name, title, and telephone number of the authorising commissioned officer;

(iii) forward the request for information by email to the Information Release Section, Services Australia (see SMCD); and

(iv) update the relevant QPRIME occurrence with:

(a) a scanned copy of the signed QP 0973; and

(b) the requested information or other advice received from Services Australia.

Authorising commissioned officers receiving a QP 0973 should:

(i) ensure that the information required is necessary to assist in the relevant investigation;

(ii) ensure all Service and other appropriate sources have been checked with a view to obtaining the required information; and

(iii) complete and endorse the 'Authorising Commissioned Officer' details on the form.

Where a 'critical request' for information is being made, the requesting officer should advise the Information Release Section, Services Australia (see SMCD) to ensure a prompt response.

7.2.4 Interstate Law Enforcement Agencies

ORDER

Before requesting inquiries be made by interstate law enforcement agencies, members are to check all available Service intelligence holdings to ensure that the required information cannot be obtained from internal sources and systems.

Requesting inquiries

When a member is investigating any matter which requires inquiries to be made in another State or Territory, that officer should furnish a report to the officer in charge for transmission to the investigating member's supervising commissioned officer. The report should:

(i) summarise the relevant facts (including copies of relevant documents);

(ii) demonstrate a basis for believing that inquiries by a particular interstate law enforcement agency will be of assistance; and

(iii) outline the nature of the information to be sought by that law enforcement agency.

A supervising commissioned officer receiving such a report should assess the need for inquiries to be made in another State or Territory. If the commissioned officer is satisfied that such inquiries are necessary, the commissioned officer should forward the report directly to the relevant interstate police establishment or to the principal officer of the relevant law enforcement agency if the appropriate establishment cannot be determined.

Requesting intelligence

Officers wishing to request intelligence from interstate law enforcement agencies are to submit an 'External Agencies Request' available on the Crime and Intelligence Command webpage on the Service Intranet.

7.2.5 Requesting information from the Commonwealth department responsible for education or employment

The Commonwealth departments responsible for education and employment keep confidential information pursuant to:

(i) the *Student Assistance Act* (Cwlth);

(ii) matters involving fraud in other government programs under the *Crimes Act* (Cwlth);

(iii) other documents relating to programs conducted by the Commonwealth departments;

(iv) job network program participants and members;

(v) various labour market programmes including work for the dole, community support transition to work and indigenous employment programs; and

(vi) other documents relating to employment.

Information held can be accessed for official purposes only in compliance with s. 6.2(d) and (e): 'Australian Privacy Principle 6–use or disclosure of personal information' of Schedule 1: 'Australian Privacy Principles' of the *Privacy Act* (Cwlth).

Officers requiring information from the Commonwealth department responsible for education or employment are to:

(i) only request information when it cannot be obtained from internal Service or other appropriate sources;

(ii) obtain authorisation from a commissioned officer to seek the requested information;

(iii) complete a Form QP 0493: 'Request for information from the Commonwealth departments responsible for education or employment'; and

(iv) send the completed QP 0493 by email to the Director, Investigations Branch, Shared Services Centre, Commonwealth Department of Education, Skills and Employment (see SMCD).

7.2.6 Request for State and Territory Police Border Alert

The Department of Home Affairs (DHA) maintains a 'Passenger Analysis, Clearance and Evaluation system' (PACE) database, which permits identification of wanted/suspect persons at the time of arrival or departure from Australia (a **'State and Territory Police Border Alert'**). The Australian Federal Police (AFP) are a Control Authority for this database.

Australian law enforcement agencies are able to request a State and Territory Police Border Alert of wanted/suspect persons who fulfil certain criteria, namely:

(i) persons wanted for or suspected of drug trafficking;

(ii) persons wanted for or suspected of customs offences;

(iii) persons who have committed serious crimes and for whom warrants are held;

(iv) persons known or suspected to be involved with terrorist organisations, supporting acts of physical violence, espionage activities or other matters of significant security interest;

(v) persons prohibited from departing Australia or wanted for offences against the *Family Law Act* (Cwlth);

(vi) persons who are subject to a Departure Prohibition Order made under the *Taxation Administration Act* (Cwlth);

(vii) persons of interest to Interpol;

(viii) other wanted or suspect persons for offences of a significant criminal nature;

(ix) persons on bail subject to conditions as:

(a) not to approach any point of international departure;

(b) not to leave Australia; or

(c) person to surrender passport/s;

(x) where a legislative power exists to take or return a person to an authorised mental health facility and a notification has been made by an authorised doctor in relation to that person. In these cases, the requesting officer is to include the name and contact details of the authorised doctor who made the original notification; and

(xi) other situations e.g. quarantine alerts.

Depending on the nature of the request and information provided by the relevant law enforcement agency, DHA or Australian Border Force officers will notify the nominated officer from the law enforcement agency of the person's movement and/or detain the person.

Officers may also consider requesting the cancellation of, refusal to issue or re-issue, an Australian passport in relation to a wanted/suspect person (see s. 7.2.7: 'Australian passports (request for information, cancellation and refusal' of this chapter).

Where a defendant has been granted bail with one of the conditions listed in (ix) above, to prevent the risk of flight by the defendant, the prosecutor appearing at the matter is to:

(i) submit an order for the surrender of the defendant's passport to the court as a condition of bail;

(ii) request the defendant not be released from custody before the surrender of the passport by either the defendant or a third party;

(iii) request an order for the defendant to remain in custody whilst the passport is returned where the defendant's third party is unable or unavailable to retrieve the passport; and

(iv) complete and submit a 'State and Territory Police Border Alert Request Form' as soon as practicable, and at a minimum prior to the termination of duty on the day of the matter appearing in court.

The Duty Officer at Police Communications Centre is the nominated on-call officer.

ORDER

The prosecutor is to ensure that the defendant's passport is surrendered prior to being released on bail.

Requesting a State and Territory Police Border Alert

Officers in charge of investigations who have reason to believe that inclusion of a person on PACE is beneficial to that investigation are to:

(i) complete a 'State and Territory Police Border Alert Request Form';

(ii) seek the approval of a commissioned officer; and

(iii) forward the completed form to the AFP in accordance with instructions provided on the form.

The PACE Alerts Officer, AFP will advise the requesting officer the information has been entered onto PACE and the period of currency.

The State and Territory Police Border Alert will remain current for a period of 90, 180 or 360 days (depending on the type of alert – as advised by the AFP) from the date advised. The alert will be deleted from the PACE system on the expiration date unless advised in writing by the officer requesting the alert be retained for a further period (as specified).

7.2.7 Australian passports (request for information, cancellation and refusal)

Officers during the course of an investigation or as part of the court process, may need to contact the Department of Foreign Affairs and Trade (DFAT) in relation to the holder of an Australian passport.

When determining bail conditions for a person who is not an Australian citizen or permanent resident, prescribed officers are to refer to s. 16.20.2: 'Prescribed police officer's (PPO) responsibilities' of the OPM.

Requesting information

Officers requiring passport information (e.g. family and given names, date of birth, other names used, validity of passport) are to submit an 'External Agency Request' available on the Crime and Intelligence Command webpage on the Service Intranet. The request is to include:

(i) the identity of the passport holder;

(ii) the reason for the request (e.g. offence being investigated including statute and section number);

(iii) whether the passport holder is a person of interest, a suspect or witness; and

(iv) the information required.

State Intelligence Group will:

(i) forward the request to DFAT; and

(ii) provide the results of the inquiry to the requesting officer.

Request for the refusal or cancellation of Australian passports

Section 12: 'Reasons relating to Australian law enforcement matters' of the *Australian Passports Act* (Cwlth), provides where a person is:

(i) the subject of an arrest warrant issued in Australia in respect to an indictable offence against the law of the Commonwealth, a State or Territory; or

(ii) prevented from travelling internationally by force of:

(a) an order of a court of the Commonwealth, a State or Territory;

(b) a condition of parole, or of a recognisance, surety, bail bond or licence for early release from prison, granted under a law of the Commonwealth, a State or Territory; or

(c) a law of the Commonwealth, or an order or other direction (however described) under a law of the Commonwealth,

an officer may make a request to the Minister for Foreign Affairs, Department of Foreign Affairs and Trade to refuse or cancel an Australian passport on law enforcement grounds.

Where officers are concerned a person may attempt to leave the country, in addition to the process contained within this section, officers should request a State and Territory Police Border Alert through the Department of Home Affairs (see s. 7.2.6: 'Request for State and Territory Police Border Alert' of this chapter).

Arrest warrants

Where an officer believes a person, the subject of an arrest warrant for an indictable offence, may attempt to leave Australia to avoid attendance at court, a request may be made to the Minister for Foreign Affairs to:

(i) have the person's current Australian passport cancelled; or

(ii) request a refusal for the issuing of, or re-issuing of an Australian passport to the person.

Persons on court bail

Where an investigating officer believes a person on bail for offences may attempt to leave Australia to avoid attendance at court, the officer should:

(i) make an application to a court for bail conditions:

(a) to prevent international travel; and

(b) if a person holds a passport, to surrender the passport to the court; and

(ii) make a request to the Minister for Foreign Affairs to:

(a) have the person's current Australian passport cancelled; or

(b) request a refusal for the issuing of, or re-issuing of an Australian passport to the person.

How to make requests

Officers are to be aware that documents submitted to DFAT to request a cancellation/refusal of an Australian Passport, may be:

(i) supplied to the subject person; or

(ii) accessible under the *Freedom of Information Act* (Cwlth).

Officers are to ensure any information that is supplied to DFAT:

(i) is not likely to interfere with the administration of justice;

(ii) is not likely to unduly interfere with the efficient and effective discharge of law enforcement duties;

(iii) is not in contravention of any statute, i.e. identify an informant; and

(iv) is not likely to interfere with or compromise any investigation.

Officers not wishing the information supplied to DFAT released to a third party may consider the use of a caveat.

Officers are to be aware that decisions made by the Minister for Foreign Affairs to refuse or cancel a passport are subject to review by the Commonwealth Administrative Appeals Tribunal.

To request the cancellation/refusal of an Australian passport of a person wanted on an arrest warrant for an indictable offence or on a bail condition that prevents international travel, the relevant officer should:

(i) for the cancellation of an Australian passport:

(a) complete a QP 0627: 'Request for the Cancellation of an Australian Passport';

(b) attach a copy of the relevant arrest warrant or court bail documents to the completed form;

(c) submit the completed documentation through the chain of command to:

- a superintendent (the contact person); and
- the Commissioner (the authorising officer),

for signature in accordance with DFAT requirements; and

(d) submit the request to the Passport Operations Section, DFAT (see SMCD); or

(e) if the request is urgent, contact DFAT Consular Emergency Centre by telephone (see SMCD); or

(ii) for a refusal to issue or a refusal to re-issue an Australian passport:

(a) complete a QP 0628: 'Request for The Refusal of An Australian Passport';

(b) attach a copy of the relevant arrest warrant or court bail documents to the completed form;

(c) submit the completed documentation through the chain of command for signature by a commissioned officer; and

(d) submit the request to:

- the Manager, DFAT, Brisbane Office (see SMCD); or
- the Brisbane Passports Office, DFAT, (see SMCD); or

(e) if the request is urgent, contact DFAT Consular Emergency Centre by telephone (see SMCD);

(iii) request a State and Territory Police Border Alert for the person (see s. 7.2.6: 'Request for State and Territory Police Border Alert' of this chapter); and

(iv) amend the relevant QPRIME occurrence with details of the request made to DFAT and upload a scanned copy of the submitted documents.

The Department of Foreign Affairs and Trade may notify the person subject of a cancellation request, prior to the decision being made by the Minister for Foreign Affairs to cancel the passport. If there is a risk that the person might attempt to travel internationally should they become aware of the request for their passport to be cancelled (before it is cancelled), officers are to provide reasons supported by an appropriate risk assessment of why the person should not be notified of the cancellation request.

The Minister for Foreign Affairs will ordinarily cancel, refuse to issue or re-issue a passport on law enforcement grounds. However, should the requesting officer not provide all the relevant information required by DFAT, including completion of the forms, the Minister may not act on the request.

Removal of passport cancellation or refusal restrictions

When the reason for the request to cancel/refuse an Australian Passport no longer exists i.e. matter is finalised through court, the requesting officer is to notify DFAT to have the passport cancellation or refusal restriction lifted.

A request for the cancellation/refusal of an Australian Passport in relation to bail conditions will automatically be removed after three years, or five years regarding arrest warrants unless a report requesting an extension is made to DFAT.

7.2.8 Requesting information from Australia Post

Officers requiring information relating to Australia Post are to ensure that all Service intelligence holdings have been thoroughly checked before any request to Australia Post is made.

Officers who require searches for Australia Post are to submit an 'External Agency Request' available on the Crime and Intelligence Command webpage on the Service Intranet. Officers are to outline in the request the following:

(i) full and correct name of person;

(ii) date of birth of person;

(iii) the address;

(iv) if known, PO Box number;

(v) town where PO Box may be located; and

(vi) why the information is being sought.

7.2.9 Requesting information from Department of Home Affairs

Search requests relating to immigration information and residency status of persons are conducted by the Department of Home Affairs (DHA).

Officers requesting information that relates to immigration information and residency status of persons should use the appropriate DHA form available on Form Select. The current forms are:

(i) 'Request for personal information'; or

(ii) 'Movement records and passenger cards request'.

The appropriate email address to send the completed forms to, is listed on each form.

See also s. 11.15.1: 'Department of Home Affairs and Australian Border Force' of the OPM.

7.3 International organisations and agencies

7.3.1 International inquiries through Interpol

Interpol is an international organisation which facilitates the exchange of information. The Commissioner of the Australian Federal Police (AFP) is the Interpol representative within Australia and the National Central Bureau of Australia (Interpol Canberra) is located at AFP Headquarters, Canberra. State Intelligence Group, Crime and Intelligence Command is the central point of contact within the Service for the information requirements for all Interpol inquiries except fingerprint records. The Fingerprint Bureau is the Service's central point of contact for Interpol inquiries for fingerprint records.

Interpol may provide assistance in facilitating the following requests:

(i) search for a wanted person with a view to their detention, arrest or restriction of movement;

(ii) locate a person or an object of interest to the police;

(iii) provide or obtain information related to a criminal investigation or to the criminal activities of a person;

(iv) warning about a person, an event, an object or a modus operandi related to criminal activities;

(v) identify a person or a deceased;

(vi) carry out forensic analyses;

(vii) perform security checks; and

(viii) identify threats, crime trends and criminal activities.

Requests for assistance from the Service to overseas law enforcement agencies

Requests for Interpol assistance to advise relatives of deceased persons are to be made in accordance with Service policy contained in s. 8.4.7: 'Advising relatives' of the OPM. Requests for Interpol assistance in relation to extraditions are to be made in accordance with Service policy contained in s. 10.9.3: 'Action prior to approval to seek extradition' of the OPM.

Requests for Interpol assistance, except fingerprint records, are to be completed by submitting an External Agency Request to State Intelligence Group (link available from State Intelligence Group page of the Service Intranet). On receipt of the request a State Intelligence Group member will forward the appropriate form to be completed by the requesting officer. Requests for fingerprint records are to be directed to the OIC, Fingerprint Bureau.

Where an inquiry is of an urgent nature, the officer is to forward an e-mail requesting Interpol assistance via the Duty Officer, Police Communications Centre. The duty officer is to ensure there is sufficient reasons outlined in the email before forwarding it.

ORDER

Members are not to contact or liaise directly with Interpol.

Information required for an external agency request

Members submitting a request in compliance with the above policy should include all relevant details pertaining to the case and the issue in question.

Generally, the following information is required:

(i) the full name of the person in the form shown on any official identification documents, and any known alias;

(ii) the person's date and place of birth, including the region, province and town;

(iii) the person's occupation, past known address and any known telephone or facsimile numbers;

(iv) whether the person's fingerprints and photograph can be supplied if necessary;

(v) names of both parents (including mother's maiden name) and their places of birth;

(vi) details of any official identification document (such as origin of passport and official number of document);

(vii) the date and place of any known international arrivals and departures and the ports from which these movements took place;

(viii) last known international place of residence; and

(ix) brief details as to the reason for the inquiry, including charges laid and the degree of urgency of the request.

The Detective Superintendent, State Intelligence Group and the Inspector in Charge, Fingerprint Bureau will cause all requests for international inquiries to be forwarded to Interpol Canberra.

Upon receipt of relevant advice from Interpol Canberra, the Detective Superintendent, State Intelligence Group, or where relevant, the Inspector in Charge, Fingerprint Bureau will cause appropriate advice to be forwarded to the requesting officer.

Action required on receipt of international criminal histories

ORDER

The State Intelligence Group member receiving an international criminal history (apart from New Zealand (NZ)) as a result of an Interpol request is to ensure they forward the result to the Police Information Centre, Information Management Services (PIC) via email to PIC.OffenderHistory. The PIC member receiving the email is to:

(i) attach the criminal history to the relevant QPRIME Person Record;

(ii) add a flag indicating the person has international criminal history; and

(iii) inform the PIC team responsible for Blue Card Services that the history has been added.

Where an investigator comes into possession of an international criminal history other than via an Interpol request they are to forward a copy via email to PIC.OffenderHistory.

For NZ criminal histories see section titled 'Requesting interstate or New Zealand criminal histories' of s. 3.7.2: 'Documentation at first appearance' of the OPM.

Requests for assistance from overseas law enforcement agencies

All requests for information and assistance received from international law enforcement agencies are to be authorised and organised through Interpol prior to any information or assistance being given by the Service. Where a request has not been authorised by or through Interpol, the assistant commissioner or a commissioned officer is to assess whether or not information or assistance is to be provided in terms of 'potential death penalty situations' prior to any assistance being given.

Potential death penalty situations

Where a request for information or assistance is received from an international law enforcement agency, and has not been authorised or organised through Interpol, before releasing information or providing assistance, officers are to determine if the request relates to a death penalty offence.

If a request does not relate to a death penalty offence, information can be released or assistance provided if appropriate, (see ss. 5.6: 'Release of information' and 5.6.15: 'Requests for information from other law enforcement agencies' of this Manual).

If the request does relate to a death penalty offence:

(i) has a person been arrested, detained, charged or convicted of an offence for which the death penalty may be imposed, if so only the relevant assistant commissioner can authorise the release of information; or

(ii) has a person been arrested, detained, charged or convicted of an offence for which the death penalty may be imposed, but there is an imminent danger to human life if the information is not provided and it is not practicable to have the matter approved by an assistant commissioner or through Interpol, have the information authorised by a commissioned officer before release; or

(iii) where no person has been arrested or detained on suspicion of having committed an offence in respect of which the death penalty may be imposed, have the information authorised by a commissioned officer before release.

If the request relates to a death penalty offence, the relevant assistant commissioner or commissioned officer before authorising the release of information to an overseas law enforcement agency is to consider the following:

(i) the purpose of providing the information;

(ii) the likelihood of the authorities in the foreign country using the information only for that purpose;

(iii) the reliability of the information;

(iv) whether the information is exculpatory in nature;

(v) nationalities of the person involved;

(vi) the persons age and personal circumstances;

(vii) the seriousness of the suspected criminal activity;

(viii) the potential risks to the person, and other persons in not providing the information;

(ix) the degree of risk to the person in providing the information including the likelihood the death penalty will be imposed;

(x) Queensland interest in promoting and securing cooperation from overseas agencies in combating crime; and

(xi) any other relevant policy including s. 5.6.15 of this Manual and ss. 2.10.1: 'The Intelligence Network', 2.23.2: 'Forensic procedure orders' and 2.25.21: 'Requesting interstate law enforcement agency for a DNA person/DNA crime scene profile or to perform a DNA comparison' of the OPM.

When releasing information to an overseas law enforcement agency, where the request has not been authorised through Interpol, officers may use QP 0854: 'Processing a request from an overseas law enforcement agency for QPS information, When the request has not been authorised through Interpol and relates to a death penalty offence'.

7.4 Business, infrastructure and service provider requests

7.4.1 Company and Business Search Requests

The Australian Securities and Investments Commission has national responsibility for business and company names.

The Australian Securities and Investments Commission website allows a search of the:

(i) company and other registers; and

(ii) the business names register,

for publicly available information.

The Australian Business Register 'ABN Lookup' website provides publicly available information supplied by businesses when they register for an Australian Business Number.

Access to Australian Securities Commission on Time (ASCOT) for company information for investigative or intelligence purposes is available to intelligence officers. This system:

(i) can provide more detailed information than the Australian Securities and Investments Commission website; however

(ii) does not produce certificates or documents for presentation in court.

Where a certificate of company registration in relation to a business or company is required for court purposes, and the business or company is the:

(i) victim in the matter, the business or company should be able to provide the certificate of company registration; or

(ii) defendant in the matter, or the legitimacy of the business name extract or company is in question, officers can make application to obtain the relevant certificates from the Australian Securities and Investments Commission.

Officers are to ensure the certificate of company registration or other business-related documents are essential to an investigation prior to making a formal request for the documents through the Australian Securities and Investments Commission.

Officers are to be aware that a business name is not an entity capable of ownership and is therefore not required to prove ownership in property offences.

Requesting information

Where an officer requires a:

(i) search of ASCOT; or

(ii) certificate of company registration or other business-related documents,

they are to submit an 'External inquiry' task within the relevant QPRIME occurrence to their local intelligence office (see SMD).

Processing requests for information

Where an intelligence officer receives a request for a search of ASCOT and the intelligence officer:

(i) has access to ASCOT, they are to conduct the search; or

(ii) does not have access to ASCOT, they are to complete the State Intelligence Group IST Request Form available on the State Intelligence Group, Crime and Intelligence Command (CIC) web page on the Service Intranet.

Where an intelligence officer receives a request for a certificate of company registration or other business-related document, the intelligence officer is to complete the State Intelligence Group IST Request Form available on the CIC web page on the Service Intranet.

7.4.2 Telecommunications information

Definitions

For the purpose of this section:

Authorised officer

means a senior officer of the Service authorised in writing by the Commissioner (see Delegation D 32.6).

Communication of telecommunications information

for chapter 2 *Telecommunications (Interception and Access) Act* (Cwlth) (TIAA) information, means any time the telecommunications information is disclosed to a person outside the Service

Disclosure of telecommunications information

for chapter 4 TIAA information, means any time the telecommunications information is communicated, given or divulged.

Enforcement agency

see s. 176A: 'Meaning of enforcement agency' of the TIAA.

Issuing authority

means a judge or a court created by Parliament, a federal magistrate, magistrate or member of the Administrative Appeals Tribunal who has consented to being appointed as an issuing authority by the Minister (see s. 6DB: 'Issuing authorities' of the TIAA).

Life threatening call

means a call connected with an event actually or potentially perilous to human life including a person being seriously injured, a bomb threat, an extortion demand, a kidnapping, a threat to public safety, and the like and which will usually require immediate call tracing action.

Source

means a person who provides information:

(i) to another person who is working in a professional capacity as a journalist; and

(ii) in the normal course of the other person's work in such a capacity; and

(iii) in the expectation that the information may be disseminated in the form of (or commentary/opinion on or analysis of) news, current affairs, or a documentary.

Stored communication

see s. 5: 'Interpretation' of the TIAA.

Unwelcome call

means a call which is of a menacing offensive or harassing nature, but which is not currently a life-threatening call, and which may be intentional or non-intentional on the part of the caller, e.g. a repeated call from an incorrectly programmed facsimile service or message bank service.

Use of telecommunications information

means use of the telecommunications information within the Service. A 'use' would include actions taken within the Service to further an investigation or to initiate and assist an unrelated investigation or in joint investigations e.g. when information is used by the Service to investigate a murder and used by the Drug Squad, CIC.

For telecommunications interception policy, see s. 2.5.10: 'Telecommunications interception' of the OPM.

Telecommunications information

Australia has a deregulated telecommunications market which means that no single carrier or on-seller possesses details of all telephone subscribers.

For the Service to obtain subscriber information, it must approach the particular carrier or on-seller providing the service to that subscriber. Some telecommunications carriers and companies act as on-sellers by buying 'air-time' from another telecommunications carrier and on-selling that 'air-time' to subscribers.

The Integrated Public Network Database (IPND) is an industry-wide database containing all listed and unlisted public telephone numbers. It is managed by Telstra under licence conditions. Part 4 of Schedule 2 of the *Telecommunications Act* (Cwlth) (TA) sets out service provider rules in relation to the IPND. Under these rules, carriage service providers (CSPs) that supply a carriage service to an end-user of a public number must provide the public number and the associated customer data to the IPND. State Intelligence Group has direct access to the Integrated Public Network Database enquiry (IPNDe) system.

State Intelligence Group, CIC maintain a contact list for all telecommunications carriers in Queensland.

The TIAA permits, under special circumstances, the disclosure of existing or prospective telecommunications information or documents to the Service.

Access to stored communications via a telecommunications carrier

In general terms, a stored communication is any kind of message (text, voice, picture, email) which has been sent over a telecommunications network and is held (stored) by a telecommunications carrier.

If the communications need to be accessed via the carrier, this may be done either:

(i) without the knowledge of the sender or recipient (i.e. covertly) with a stored communications warrant issued under Chapter 3: 'Preserving and accessing stored communications' of the TIAA. A stored communications warrant may only be applied for in relation to a suspect or a victim where the victim is unable to consent, or it is impracticable for the victim to consent. In all instances, a stored communications warrant will only be issued where an issuing authority is satisfied the information likely to be obtained is likely to assist with the investigation of an offence punishable by at least three-years imprisonment or an offence committed by an individual punishable by a fine of at least 180 penalty units or if the offence cannot be committed by an individual, a fine of at least 900 penalty units; or

(ii) with the knowledge of the sender or recipient with a conventional search warrant issued under the PPRA.

Stored communications are only held by telecommunications carriers for a short period of time before being deleted.

Officers wishing to access stored communications via a telecommunications carrier are to firstly request the information be preserved by:

(i) completing the relevant preservation request form as soon as practicable (available from the Crime and Intelligence Legal Services, Legal Division webpage of the Service Intranet);

(ii) contacting the Crime and Intelligence Legal Services prior to submitting the preservation request; and

(iii) submitting the preservation request to the Telecommunications Interception Unit, Covert and Specialist Operations Group, Operations Support Command for processing.

To make an application for a stored communications warrant, officers are to contact the Crime and Intelligence Legal Services, Legal Division, who will provide the affidavit pro forma. Officers are to complete a draft of the affidavit and return it to the Crime and Intelligence Legal Services, where a legal officer will:

(i) review the affidavit;

(ii) liaise with the investigating officer to ensure the affidavit meets the criteria set out in legislation; and

(iii) once satisfied that the affidavit is sufficient, a legal officer from the CIC Legal Unit, Legal Division will make application for the stored communications warrant to an issuing authority.

Section 119: 'Duration of stored communications warrants' of the TIAA provides that a stored communications warrant is in force until it is first executed, or five days after the day on which it was issued, whichever occurs first.

If access to stored communications is to be made with the knowledge of the sender or recipient, officers are to:

(i) serve a 'Notice of Intention' (available on the Crime and Intelligence Legal Services webpage) on the sender or recipient; and

(ii) submit the 'Notice of Intention' with the preservation request to the Telecommunications Interception Unit,

prior to applying for a search warrant to access the data from the carrier. In some circumstances, the stored communications will not be available in Queensland, and arrangements will need to be made to obtain a search warrant interstate. For the procedure to obtain an interstate warrant see s. 4.11.1: 'When Queensland is the receiving State' of the OPM.

Access to stored communications without the assistance of a telecommunications carrier

Police can also use relevant powers under the PPRA to access a communication without the assistance of the carrier, e.g. accessing a SMS by using a suspect's mobile phone.

Powers under the PPRA which would allow access to a stored communication include:

(i) s. 29: 'Searching persons without warrant';

(ii) s. 31: 'Searching vehicles without warrant';

(iii) s. 154: 'Order in search warrant about device information from digital device', and

(iv) s. 157: 'Powers under search warrant'.

These powers in various circumstances provide officers with the ability to search a person's property (e.g. phone or computer) and access communications that are available and accessible to that property.

As an example of s. 29: 'Searching persons without warrant' of the PPRA, where an officer reasonably suspects a prescribed circumstance under s. 30: 'Prescribed circumstances for searching persons without warrant' of the Act exists, the officer may stop and detain the person without warrant and in accordance with s. 29(1)(b) search the person and anything in the person's possession for anything relevant to the circumstances for which the person is detained.

The officer who has stopped and detained a person for the purpose of searching the person without warrant may locate a mobile phone and access any information already stored or contained in the mobile phone e.g. SMS, voicemail messages and draft messages not yet sent, the only proviso is that the information is stored on the mobile phone.

Additionally, as an example of a search in accordance with s. 157 of the PPRA, where an officer has executed a search warrant under the provisions of the Act and pursuant to the search warrant the officer searches a person and locates a mobile phone, the officer has the power within the provisions of the search warrant to search through the person's mobile phone and is authorised to retrieve a communication.

When an officer is utilising a power under the PPRA to search a person's property to access communications, the officer is entitled to access a communication once it is available for the intended recipient to access it. It is irrelevant whether or not the suspect has accessed that communication themselves.

Where property has been seized and an examination of the device is required, see also s. 2.6.10: 'Electronic evidence examination' of the OPM.

Access to telecommunications data information

Chapter 4: 'Access to telecommunications data' of the TIAA provides provisions for both historical and prospective data information. It is important to recognise that any information requested is to be approved by an authorised officer (see 'Definitions' of this section).

Section 178: 'Authorisations for access to existing information or documents – enforcement of the criminal law' of the TIAA allows for information to be disclosed to any member of the Service if the request for that information is reasonably necessary for the enforcement of the criminal law. This applies during a criminal investigation.

Section 178A: 'Authorisations for access to existing information or documents – locating missing persons' of the TIAA allows for information to be disclosed to any member of the Service if reasonably necessary for the purposes of finding a missing person. Information obtained under s. 178A of the TIAA is for the purpose of locating a missing person and is not to be used for other routine criminal investigations.

Section 179: 'Authorisations for access to existing information or documents – enforcement of a law imposing a pecuniary penalty or protection of the public revenue' of the TIAA allows for the same provisions as s. 178 of the Act, however this section relates to offences which are punishable by a pecuniary penalty order or for the purpose of protecting public revenue.

Officers who wish to make a request for telecommunications information from a telecommunications carrier are to ensure that:

(i) the information required cannot be obtained lawfully from QPRIME, a telephone directory, or directory assistance; and

(ii) all reasonable steps have been taken to ascertain which telecommunications carrier would be able to supply the information sought.

Where an officer requires existing telecommunication information e.g. Integrated Public Network Database enquiry (IPNDe), subscriber or Call Charge Records (CCR) or Reverse Call Charge Records (RCCR), they are to:

(i) complete a QP 1031: 'Application for authorisation and notification for access to existing information or documents - IPNDe' or QP 1032: 'Application for authorisation and notification for access to existing information or documents - CCR' as relevant;

(ii) upload QP 1031 or QP 1032 into the relevant QPRIME occurrence and send a 'Telecommunications request' task to the Intelligence Support Team, State Intelligence Group [ORG unit 3064] for processing; and

(iii) if applicable, ensure that the Intelligence Support Team, State Intelligence Group [ORG Unit 3064] is included in the custom ACL group placed on the QPRIME occurrence, to allow processing of tasks. Any exception to this is to be approved by the Detective Inspector (Specialist Operations), State Intelligence Group.

For further information regarding Telecommunications Requests, see 'Requesting Historical Telecommunications Data' on the State Intelligence Group webpage of the Service Intranet.

Section 180: 'Authorisations for access to prospective information or documents' of the TIAA allows for prospective telecommunication information to be disclosed to the Service. This section applies to information received during the authorisation period of up to forty-five days and only applies to offences that carry a minimum 3 year offence penalty.

Officers wishing to make an application for prospective data in accordance with s. 180 of the TIAA are to:

(i) complete a 'Request for access to prospective information or documents' on IMAC providing sufficient information required to support a prospective data application;

(ii) obtain and upload relevant subscriber or IPNDe check (no more than five business days old) on IMAC; and

(iii) submit the Request for Access to prospective information or documents on IMAC to their relevant authorised officer for consideration.

The relevant authorised officer, once satisfied the disclosure of information sought is reasonably necessary for the investigation of the nominated offence meets all legislative requirements of the Act, may approve the Request for Access to prospective information or documents on IMAC.

Authorisation thresholds, use and disclosure of telecommunications information

Authorised officers are required to satisfy a proportionality test under the TIAA when making telecommunications information authorisations, which will ensure that the scheme for accessing telecommunications data under the TIAA:

(i) addresses the needs of enforcement agencies when carrying out their functions and activities using the least privacy intrusive means possible; and

(ii) is consistent with community expectations about the handling of personal information.

The TIAA requires agencies to keep records associated with the use and disclosure of telecommunication information (see 'Definitions' of this section). The Service will be subject to annual inspections regarding the use of powers under

the TIAA by the Commonwealth Ombudsman, as well as reporting to the Commonwealth Attorney-General's department.

For prospective data use, officers are to comply with the 'Prospective Data Authorisations' webpage on the Telecommunications Interception Unit site on the Service Intranet.

For IPNDe, subscriber or call charge records, officers are to make a record of the use and disclosure of telecommunications information within QPRIME (see 'Telecommunications Requests' on the State Intelligence Group webpage on the Service Intranet). For sensitive investigations, this record in QPRIME can reference another location that contains the details (e.g. diary notes) that can be accessed for any required inspection.

ORDER

Before making an authorisation, authorising officers are to be satisfied on reasonable grounds any interference with the privacy that may result from the disclosure or use of telecommunications information is justifiable and proportionate having regard to a number of factors (see s. 180F: 'Authorised officers to consider privacy' of the TIAA).

In accordance with the TIAA, authorising officers are not to make an authorisation that would authorise the disclosure of information or documents relating to a particular person if the authorised officer knows or reasonably believes a particular person to be a person who is working in a professional capacity as a journalist or an employer of a person, and a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source, unless a journalist information warrant is in force in relation to the particular person. For further information, officers may contact the Crime and Intelligence Legal Services, Legal Division.

Unwelcome calls

Telephone calls of a menacing, offensive or harassing nature that are received and are not of a life-threatening nature are classed as unwelcome calls (see 'Definitions' of this section) and members are to:

(i) advise complainants to contact their telecommunications carrier; or

(ii) investigate the matter,

as the circumstances warrant.

Officers investigating a complaint of improper use of a telecommunications service are to establish;

(i) the relevant statute law breached or the details of the serious and imminent threat to life or health of a person; and

(ii) whether a trace facility is presently installed on the relevant land line telephone service.

Where a member of the public has reported the unwelcome calls to their telecommunication carrier, officers may be able to obtain the details of the unwelcome calls through the carrier by providing the unwelcome calls reference number (usually with no cost) or obtain call charge records in accordance with normal procedure.

Where the unwelcome call is in relation to an event actually or potentially perilous to human life including a person being seriously injured, a bomb threat, an extortion demand, a kidnapping, a threat to public safety which requires immediate call tracing action are to direct their inquiries to the Duty Officer, Brisbane Police Communications Centre (BPCC).

Serious and imminent threat to persons life or health

Where there is a serious and imminent threat to the life or health of a person in accordance with s. 287 of the TA:

(i) Duty Officers at BPCC; or

(ii) who has been assessed as a High-Risk Missing Person (see definitions in s. 12.1: 'Missing Persons' of the OPM) by the Detective Inspector, Detective Senior Sergeant or Operations Leader, Missing Persons Unit (Homicide Investigation Unit),

may, through telephone service providers, perform one or more of the following checks:

(i) emergency life-threatening trace (e.g. call made re bomb on train; call to Kids Helpline or Lifeline where a person is threatening suicide);

(ii) mobile phone triangulation (e.g. suicidal person when whereabouts unknown);

(iii) customer details (e.g. when a trace locates a phone number and the person's identity is unknown);

(iv) CCR or RCCR (e.g. when knowledge of who is communicating with the subject person may assist in preventing or reducing serious and imminent threat to the life or health of a person); and

(v) email, internet chat rooms or voice over internet protocol (VOIP) (e.g. person threatening suicide via e-mail, or social media platforms).

Section 315: 'Suspension of supply of carriage service in an emergency' of the TA provides the power to suspend the supply of a carriage service in an emergency. Where a suspension of carriage service is required, such as a siege situation or police negotiations, duty officers at PCC can assist by providing line isolation. Prior to contacting PCC to

obtain line isolation in accordance with s. 315 of the TA, officers are to seek the approval of the assistant commissioner of the incident region.

Authorising officers are to be satisfied that the request is:

(i) reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person; and

(ii) for the purpose as stated in s. 315 of the TA.

7.4.3 Retail energy providers

Definitions

For the purpose of this section:

Authorising officers

are officers who can authorise a request for retail energy provider customer information.

The following are authorising officers:

(i) senior sergeants, State Intelligence Group, Crime and Intelligence Command;

(ii) regional intelligence and strategy officers;

(iii) commissioned officers; or

(iv) OICs of district intelligence offices.

Inquiring officers

are officers seeking retail energy provider customer information.

Requesting officers

are officers authorised to request information from retail energy providers. For the purposes of this section, all members appointed by the Service as an intelligence officer/analyst are authorised to request information from providers.

Retail energy providers

Requests for information held by retail energy providers may be made when it is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty and only when all reasonable alternative avenues for seeking the information have been exhausted.

Inquiring officers are to exhaust all Service information/intelligence sources available to them prior to submitting an 'External inquiry' task within the relevant QPRIME occurrence to their local intelligence office (see SMD).

If the required information is not available from the in-Service information/intelligence holdings the requesting officer should obtain authority from their relevant authorising officer to commence a retail energy provider customer information search through their local intelligence office.

Authorising officers are to ensure that all Service information/intelligence sources available to them have been exhausted before authorising a request for retail energy provider customer information.

The requesting officer is to complete a request for information from within QPRIME, including the authorising officer's details. The requesting officer is to email:

(i) the target address details to Energex, who will provide the details of the retail energy provider to the requesting officer; and

(ii) the request form to the relevant retail energy provider.

Emergent after-hours requests

Requesting officers who require retail energy provider customer information after-hours in emergent circumstances are to contact the State Intelligence Group, Crime and Intelligence Command for retail energy provider contact information.

7.4.4 Requesting information from financial institutions

In accordance with s. 197B: 'Giving notice to financial institution' of the *Police Powers and Responsibilities Act*, a senior police officer (of the rank of inspector or above) may give a QP 0968: 'Financial institution account information notice' to a financial institution, if the officer:

(i) reasonably suspects an offence:

(a) has been committed;

(b) is being committed; or

(c) is about to be committed; and

(ii) reasonably believes the information sought from the financial institution is required for:

(a) investigating the offence;

(b) commencing proceedings against a person for the offence; or

(c) taking steps reasonably necessary to prevent the commission of the offence.

A financial institution receiving a QP 0968 must, when a:

(i) name is provided, state whether a named person is or was authorised to operate an account with the financial institution; or

(ii) number is provided, state whether an account with the stated number is or was held at any time with the financial institution, and

provide the details of the account and the names of persons who held or were authorised to operate the account within a stated reasonable time (see ss. 197B and 197D: 'Financial institution must comply with notice' of the *Police Powers and Responsibilities Act*).

Conducting these searches will only retrieve information relating to whether a person holds or operates an account. Account statements and details will not be supplied. If an officer is requiring this information, a search warrant or a QP 0716: 'Production notice' will need to be obtained (see s. 2.8.12: 'Production notices and access orders' of the Operational Procedures Manual).

A list of financial institutions is available on the Financial and Cyber Crime Group's webpage on the Service Intranet.

Officers requiring searches of account holders from financial institutions are to:

(i) obtain approval from a senior police officer after providing sufficient information to develop the reasonable belief that a notice to a financial institution is necessary;

(ii) complete and save the QP 0968 in the relevant QPRIME occurrence; and

(iii) forward the completed QP 0968 to the financial institution(s) in accordance with the instructions on the form.

The results of the inquiry will be forwarded directly to the investigating officer by the financial institutions. Officers receiving financial institution results are to:

(i) update the relevant QPRIME occurrence with the results;

(ii) check off financial institutions who have replied to ensure all financial institutions listed on the Fraud and Cyber Crime Group web page respond; and

(iii) perform follow-up inquiries with any listed financial institutions that have failed to respond within the specified period for any reason why the notice was not complied with.

ORDER

Officers investigating an offence under the *Police Powers and Responsibilities Act* are to provide sufficient information to the commissioned officer for them to form a reasonable belief to support the provision of a QP 0968 to a financial institution.

Where a QP 0968 is given to a financial institution, the commissioned officer seeking the information is to make a written record in their official police notebook or diary of their reasonable suspicion and belief required under s. 197B(1): 'Giving notice to financial institution' of the *Police Powers and Responsibilities Act*.

7.4.5 Requesting information from social media providers (including Uber)

Social media platforms may be used to commit or provide evidence of an offence. Social media providers are private companies and information will only be provided in accordance with the legal process in the provider's country.

Social media providers have individual requirements for the release of information to law enforcement agencies, which are usually available on the relevant website. Social media provider 'Law enforcement guidelines' are reproduced on the Crime and Intelligence Command (CIC) Information Hub webpage on the Service Intranet. Requirements for Uber are contained in s. 2.28.4 of the OPM.

Information published on social media accounts consists of:

(i) non-content data, which relates to basic subscriber information, such as:

(a) the account user-id;

(b) email address(es);

(c) Internet Protocol (IP) logs; and

(d) the date and time the relevant account was created; and

(ii) content data which will include messages, published posts, photographs etc.

Officers should be aware that social media content can rapidly change as account users can modify or delete information.

The collection of data from social media providers can be a long process. Officers are to, where practicable, obtain a copy of relevant published information (by the victim or Service member download or screen-shot etc.) at the earliest opportunity (see s. 2.10.6: 'Online intelligence' of the OPM).

In some instances, providers will only provide information to specific officers or units, generally within CIC.

Where information is downloaded or copied from a social media platform, the investigating officer is to:

(i) make a record of the relevant information in their official police notebook or official diary; and

(ii) where practicable, save information in the relevant QPRIME occurrence with information such as the IP address and date and time the information was obtained.

Sensitive evidence (see s. 590AF: 'Meaning of sensitive evidence' of the CC) is not to be stored in QPRIME.

Obtaining information urgently

Social media providers will generally provide limited information when law enforcement agencies have received information about an imminent risk of a:

(i) child suffering abuse; or

(ii) person suffering death or serious injury,

which has been publicised on a social media website/platform.

Information on how to request urgent information is on the relevant social media website. The social media provider will outline the information which must be provided, which may involve a web-form or email-based application from a Service email address and may require a covering letter on Service letterhead.

Where information is received of an imminent risk which has been published on social media, officers are to commence an investigation, particularly to identify the whereabouts of the person at risk (see s. 2.5: 'Investigation' of the OPM).

Whenever practicable, all Service database inquiries are to be exhausted prior to making application to a social media provider.

Urgent requests for non-content data are to be made by:

(i) submitting an 'External Agency Request' (available on the State Intelligence Group webpage on the Service Intranet); and

(ii) request the relevant intelligence office to contact the Intelligence Support Team, State Intelligence to prioritise the matter.

Obtaining non-content data from social media providers

Non-content data from social media may assist investigating officers to identify the publisher of the relevant information. Non-content data is generally only provided for investigatory purposes and usually cannot be introduced as evidence in court.

Where non-content data will be required for court presentation, an evidence certificate and statement of witness will be required, and a mutual assistance request is to be made in accordance with subsection 'Obtaining content data from social media providers' of this section.

Where non-content data is sought for an investigation, officers are to submit an 'External Agency Request' available on the State Intelligence Group webpage on the Service Intranet.

Obtaining content data from foreign social media providers

Where an application for content data is required, the investigating officer is to make application for a 'data preservation request' (see the CIC Command and Administration Guides webpage on the Service Intranet) as early as possible. The request will save all information published in the relevant account at a specific point in time. Preserved data will be held for a set period (e.g. Facebook preserves data for 90 or 180 days) and will be released on receipt of an approved mutual assistance request. Applications are submitted as a mutual assistance request through the Australian Attorney-General's Department in accordance with the *Mutual Assistance in Criminal Matters Act* (Cwlth).

Where content data from a foreign social media provider is required, a mutual assistance request is to be made through the Australian Attorney-General's Department in accordance with the *Mutual Assistance in Criminal Matters Act* (Cwlth) to the relevant nation.

Where information is sought from a foreign social media provider, investigating officers are to comply with the directions contained on the CIC Information Hub webpage on the Service Intranet.

7.4.6 Requesting information from domestic airlines

QANTAS and Jetstar Airlines

Officers who require information from Qantas or Jetstar Airlines for an investigation are to ensure that all Service intelligence holdings have been thoroughly checked prior to making any requests.

Officers who require information from Qantas Airlines and Jetstar Airlines are to submit an 'External Agency Request' available on the State Intelligence Group webpage on the Service Intranet.

Officers are to outline the following on the request:

(i) name of the person;

(ii) flight details if known;

(iii) expected travel times and dates if known; and

(iv) point of origin and destination if known.

Virgin Australia Airlines (non-urgent and any inquiries during office hours)

Officers who require information from Virgin Australia Airlines for an investigation are to ensure that all Service intelligence holdings have been thoroughly checked prior to making any requests.

Officers requesting non-urgent information or any inquiries during office hours (9am-5pm Monday-Friday) are to:

(i) complete a 'Virgin Australia Law Enforcement Information Request' form available on the CIC Information Hub webpage on the Service Intranet;

(ii) obtain expenditure approval from an authorised officer. The authorising officer must be copied in the e-mail when forwarding the request; and

(iii) submit the form via e-mail to **SIGQPOL@police.qld.gov.au**.

Virgin Australia Airlines (urgent outside of office hours inquiries)

For urgent information required outside of office hours, requesting officers are to:

(i) complete a 'Virgin Australia Law Enforcement Information Request' form available on the CIC Information Hub webpage on the Service Intranet;

(ii) attend the airport in person;

(iii) contact the:

(a) guest services shift supervisor; or

(b) Virgin Australia Airport Manager;

(iv) produce their Service identification; and

(v) supply a completed and authorised 'Virgin Australia Law Enforcement Information Request Form' to Virgin staff.

Further information and required forms are located on the CIC Information Hub webpage on the Service Intranet.

7.4.7 Requesting information from tolling records

Transurban's National Enforcement Team manage Queensland Police inquiries in relation to requests for tolling records related to law enforcement purposes.

In order to comply with Transurban's privacy obligations, members requesting information are to complete a QP 1131: 'Transurban disclosure form' and submit via email to policerequests@transurban.com to enable the release of tolling records.