



**Office of the Information Commissioner**  
Queensland

**Disclosure of Personal Information**

Review of TransLink's disclosure of go card information to the  
Queensland Police Service



This report to the Queensland Legislative Assembly by the Office of the Information Commissioner is licensed under a Creative Commons - Attribution Non Commercial No Derivatives 3.0 Unported License. People reading or using this report may do so in accordance with the following conditions: Attribution (BY), requiring attribution to the original author; Non-Commercial (NC), requiring the work is not used for commercial purposes; and No Derivative Works (ND), allowing only the original work, without derivatives.

© The State of Queensland. (Office of the Information Commissioner) 2010

Copies of this report are available on our website at [www.oic.qld.gov.au](http://www.oic.qld.gov.au) and further copies are available on request to:

Office of the Information Commissioner  
Level 8, 160 Mary Street, Brisbane, Qld 4000  
PO Box 10143, Adelaide Street, Brisbane, Qld 4000  
Phone 07 3234 7373  
Fax 07 3405 1122  
Email [administration@oic.qld.gov.au](mailto:administration@oic.qld.gov.au)  
Web [www.oic.qld.gov.au](http://www.oic.qld.gov.au)

ISBN: 978-0-646-54764-0

November 2010

The Honourable R John Mickel MP  
Speaker of the Legislative Assembly  
Parliament House  
George Street  
BRISBANE Q 4000

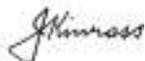
Dear Mr Speaker

I am pleased to present the Disclosure of Personal Information: Review of TransLink's disclosure of *go* card information to the Queensland Police Service. This report is prepared under section 135 of the *Information Privacy Act 2009*.

The report reviews personal information handling practices, in particular compliance with Information Privacy Principle 11 (Limits on disclosure), which agencies are required to adopt under section 27 of the *Information Privacy Act 2009*.

In accordance with subsection 193(5) of the Act, I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely



Julie Kinross  
**Information Commissioner**



## Table of Contents

1	Executive Summary .....	1
2	Recommendations .....	3
3	Why was this review done? .....	5
4	What is a <i>go card</i> ? .....	6
5	What does the law say?.....	9
6	How was the review done? .....	11
7	Timeline of the review.....	12
8	Requests for <i>go card</i> information .....	14
9	What did the review find?.....	17
10	How is <i>go card</i> information managed? .....	24
	<b>APPENDICES.....</b>	<b>31</b>
	Appendix 1 – Terms of Reference .....	33
	Appendix 2 – Glossary .....	37
	Appendix 3 – Detail and breakdown of pre-review requests.....	41
	Appendix 4 – Detail and breakdown of post-review requests.....	55
	Appendix 5 – Request Form.....	57
	Appendix 6 – <i>go card</i> retail outlets .....	61
	Appendix 7 – TransLink’s Online Privacy Statement .....	63

## **ACKNOWLEDGEMENTS**

OIC would like to thank the staff of TransLink and the Queensland Police Service for their cooperation throughout the review process and their courteous conduct.

# 1 Executive Summary

---

On 29 July 2010, the Brisbane Times reported the Queensland Police Service had used *go* card records to track down a woman who might have been a witness in a murder investigation. *Go* card is the electronic ticketing system used in South East Queensland and is administered by the TransLink Transit Authority (TransLink).

On 30 July 2010 the Privacy Commissioner announced a review into the handling of personal information contained in *go* cards and its disclosure to the Queensland Police Service.

This review found the Queensland Police Service had asked TransLink for personal information from the *go* card database to assist in law enforcement investigations and to locate missing persons. It also found that TransLink had provided some personal information in response.

The Queensland Police Service and TransLink have obligations under the *Information Privacy Act 2009* with respect to the collection, use and disclosure of personal information. Nothing in the Information Privacy Act compels TransLink to provide personal information to a law enforcement agency. However, if TransLink decides to exercise its discretion to disclose personal information to a law enforcement agency, it can do so if it is satisfied on reasonable grounds that the disclosure is necessary:

- for the prevention, detection, investigation, prosecution or punishment of criminal offences or other breaches of the law, 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.

The review examined 55 Queensland Police Service investigations seeking *go* card information, where requests were received prior to the commencement of the review, and a further 16 requests for information received after the review commenced. These requests concerned 142 *go* cards.

A clear picture has emerged. The requests for *go* card information made prior to the commencement of the review were not handled in accordance with the requirements of the Information Privacy Act on a number of occasions.

In most cases when TransLink disclosed information it did not have sufficient information to satisfy itself under the Information Privacy Act that the disclosure was necessary.

The requests made after the commencement of the review, which were made using new procedures and a structured form developed by TransLink, were generally handled in accordance with the Information Privacy Act. The new system improved the communication from the Queensland Police Service about the reason for the request, provided better authorisation for making the request and, on the small sample reviewed, achieved a quicker result.

TransLink has developed policies and business strategies to ensure that future requests from the Queensland Police Service are considered, recorded and properly authorised through a central coordination unit, applying rigorous policies and procedures.

In accordance with the Terms of Reference, the review identified general privacy issues related to the handling of *go* card information which are outlined in Part 10.

The Office of the Information Commissioner (OIC) received co-operation throughout the review, and was encouraged by the efforts made by TransLink and the Queensland Police Service to respond to the issues and address them.

Both TransLink and Queensland Police Service provided a formal response to the OIC's report and this was taken into account when finalising the report. Both agencies supported the recommendations in the report.

OIC will assess the implementation of the recommendations of this report by TransLink and the Queensland Police Service six months from the date of the report.

## 2 Recommendations

---

### Recommendation One

TransLink only disclose personal *go* card information to the Queensland Police Service (QPS) under IPP 11(1)(c) or (e) if it has:

- a) sufficient information about QPS' investigation to satisfy itself on reasonable grounds that the disclosure is necessary, or
- b) been satisfied by QPS in another way, for example, through discussion between a QPS officer and a specified TransLink officer, who then notes on the TransLink record that they are satisfied that the information is necessary for a law enforcement activity and can be disclosed.

### Recommendation Two

QPS limit its requests to the specific personal *go* card information necessary for QPS' investigation. Where necessary, QPS and TransLink should work together to clarify the scope of the request to limit the disclosure to the specific information necessary.

### Recommendation Three

- a) TransLink ensure that when *go* card information is disclosed to a law enforcement agency a note to that effect is added to the *go* card database (the Nextfare system) as soon as practicable.
- b) TransLink add such a note to any *go* card information which has previously been disclosed within three months from the date of this report.

### Recommendation Four

TransLink and QPS use the *Queensland Police Service Information Request* form when QPS is requesting information from TransLink.

### Recommendation Five

Requests for personal *go* card information should be co-signed by a more senior QPS officer to the one making the request.

### Recommendation Six

TransLink should update its Privacy Statement to state that information may be disclosed where it is "authorised or required by law".

## Recommendation Seven

TransLink and QPS should ensure clear policies, systems and procedures are implemented to raise awareness of, and require compliance with, personal information handling practices to meet requirements of the IP Act. This includes the following:

- a) TransLink's draft policies and procedures document *Managing Information Privacy* is formalised;
- b) a clear and consistent process for managing TransLink's privacy matters is put in place;
- c) all the personal information collected for *go* cards is necessary, relevant and consistent across the registration methods; and
- d) TransLink establish a high level of data security in systems for accessing Nextfare, processing hard copy registration forms, and managing complaints.

### 3 Why was this review done?

---

On 29 July 2010, the Brisbane Times reported Queensland Police Service (QPS) had used *go* card records to contact a woman who might have been a witness in a murder investigation. The article stated:

*The woman, who wished to remain anonymous, said she felt rattled when called by a detective seeking information on a bus trip she'd taken in New Farm three weeks earlier.*

*Her unease grew when the officer also revealed the name of her partner.*

The article revealed that police sought access to information in the database used by TransLink which holds personal details of people who had purchased a *go* card. *Go* cards are electronic tickets in the form of a plastic card which allow travel by bus, train or ferry in South East Queensland.

The report generated a strong community response. The Brisbane Times ran an online poll about the privacy of *go* card users. 3164 people voted. 64% of these respondents stated that they were concerned about the privacy of *go* card users.<sup>1</sup>

This report was picked up in the national media, for example, by the Sydney Morning Herald,<sup>2</sup> and resulted in public comment from the Commissioner of Police,<sup>3</sup> TransLink, other government figures and civil libertarians.<sup>4</sup>

On 30 July 2010 the Privacy Commissioner announced a review into the handling of *go* card information.

---

<sup>1</sup> <http://www.brisbanetimes.com.au/polls/queensland/go-card-privacy/20100729-10wdq.html>

<sup>2</sup> <http://news.smh.com.au/breaking-news-national/go-cards-help-police-investigate-murder-20100729-10wk6.html>

<sup>3</sup> <http://www.brisbanetimes.com.au/queensland/atkinson-to-ask-privacy-commissioner-not-to-cut-access-to-go-cards-20100801-1116i.html>

<sup>4</sup> <http://www.brisbanetimes.com.au/queensland/privacy-commissioner-launches-go-card-review-20100730-10z7n.html>

## 4 What is a go card?

---

### 4.1 The go card system

TransLink provides a public transport network for people to travel by bus, train or ferry in South East Queensland. The go card is TransLink's electronic ticket for use throughout the network. The go card can store a credit balance up to \$250 per card and each go card records travel and purchase details. There are four types of go card: an adult go card and three types of go cards offering concession fares to seniors, children, students, pensioners and defence force veterans.

As at August 2010, a go card could be purchased for \$10<sup>5</sup>, from any one of 656 retail outlets, including convenience stores, newsagents, and railway ticket offices. Once purchased with a minimum starting balance a go card can be used immediately. Go card balances can be topped up at retailers, fare machines or railway ticket offices and some private TransLink bus operators. If registered, a go card can be topped up online or by phone, or by setting up an automatic top-up facility.

To use a go card at the start of a journey, a passenger "touches on". At the end of the journey, the passenger "touches off". The details of the journey are recorded and the cost of the journey deducted from the go card balance. If a go card is not touched on at the start of a journey or touched off at the end of the journey, it is updated automatically at the next usage and a standard fee deducted from the credit balance.

### 4.2 Information in the go card system

Information stored on the go card itself is:

- a unique 16 digit go card identification number;
- the remaining credit available on the go card to pay for travel fares;
- whether or not the go card is currently touched on or off;
- if activated, an auto top-up facility that automatically increases the go card credit balance to a pre-set amount if it falls below \$5; and
- a history of the last 10 trips, showing the time, date and the start and end location.

---

<sup>5</sup> Made up of a \$5 refundable deposit and a \$5 starting balance.

### 4.3 Registration of go cards

Go cards can be registered online, by phone, by mail or in person. To register a go card, a go card holder sends personal information to the go card system (Nextfare) to register the go card in his or her name. If a registered go card is lost or stolen, the go card holder can contact TransLink, who will “hotlist” the go card, so that it can no longer be used for travel. Registration protects the go card and its credit balance in case of loss or theft and gives access to additional services, for example, automatic top-up of the go card balance.

The information required for online registration is:

- Card holder contact information
  - Phone number (fax, home, mobile or work)
  - Email address
  - Online password
  - A cardholder question and answer
- Authorised user postal address
  - First name
  - Middle initial (not mandatory)
  - Last name
  - Address lines 1 and 2 (Line 2 is not mandatory), Suburb, State and Postcode.

The information sought for registration over the phone is similar. A go card holder must provide their name, address and a contact phone number and is also asked for an additional contact phone number. The go card holder must also adopt a security question (for example, their mother’s maiden name) and is advised that he or she has the option to ask for a password to be set up. The call centre operators who register go cards over the phone enter this information directly into Nextfare.

The hard copy registration form requires similar but not identical information. For example, it requires a home address and postal address (if different to the home address) for cardholders, and a daytime phone number. It prompts for date of birth for cardholders and authorised users, which does not happen for online registration. The hard copy form also seeks credit card details which is not the case for online registration.

People seeking a concession *go* card are asked to provide the card number and expiry date of the relevant concession card (pensioner, student, senior or veteran card). Children are asked for their date of birth, but proof of age is not required.

## 5 What does the law say?

---

### 5.1 Does the *Information Privacy Act 2009* apply?

TransLink is a statutory authority falling within the definition of “public authority” in section 21 of the IP Act, and the Queensland Police Service (QPS) is a department. Both are agencies as defined in section 18 of the *Information Privacy Act 2009* (IP Act), and are required to comply with the IP Act.

Section 135(1)(a) of the IP Act gives the Information Commissioner the power to conduct reviews into the personal information handling practices of agencies and report the findings to Parliament.

### 5.2 Is the *go card* information personal information?

The IP Act provides safeguards for the handling of personal information. Personal information is defined in section 12 of the IP Act:

*Personal information is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably be ascertained, from the information or opinion.*

When a *go card* is registered, TransLink collects personal information from *go card* holders, including their name, address, telephone number and other contact details. These details, and other information such as the travel history of the *go card*, are captured in the *go card* database, the Nextfare system. If a *go card* is registered, all the information in the Nextfare system and on the *go card* itself is information about an individual whose identity can be reasonably ascertained; all the information is personal information.

Unregistered *go cards* can also be linked to personal information. A travel history is recorded for unregistered *go cards*. This means that if a person can be linked to an unregistered *go card*, for example, if the *go card* is on their person and they state that they have been using the *go card*, then all the information in the Nextfare system and on the *go card* is personal information.

### **5.3 Is giving go card information to QPS a disclosure?**

Section 23 of the IP Act defines disclosure. An agency discloses personal information if it gives it to someone who does not already know it and the agency will not be able to control what that person does with it. TransLink is disclosing personal information when it releases go card information to QPS.

### **5.4 What does the IP Act require?**

No provision in the IP Act compels TransLink to provide personal information to law enforcement agencies. If an agency such as TransLink decides to exercise its discretion to provide personal information, it must ensure it complies with the IP Act in doing so.

Section 27 of the IP Act requires agencies<sup>6</sup> to comply with the 11 Information Privacy Principles (IPPs) set out in Schedule 3 when handling personal information.

The main focus of the review has been on Information Privacy Principle 11 (IPP 11), which provides that an agency must not disclose personal information to an entity other than the individual concerned, unless one of six exemptions applies. Two exemptions are particularly relevant to the review:

- IPP 11(1)(c) which allows personal information to be disclosed to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; and
- IPP 11(1)(e)(i) which allows personal information to be disclosed to a law enforcement agency if the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions, by or for a law enforcement agency.

### **5.5 Is QPS a law enforcement agency under the IP Act?**

Schedule 5 of the IP Act states that a law enforcement agency includes the Queensland Police Service under the *Police Services Administration Act 1990*.

---

<sup>6</sup> Note that this applies to all agencies except Queensland Health, which is subject to the National Privacy Principles in Schedule 4.

## 6 How was the review done?

---

Terms of Reference for the review were sent to the Commissioner for Police and the Chief Executive Officer of TransLink on 30 July 2010. These are set out in Appendix 1. In particular, the review sought to establish that:

- each time TransLink disclosed *go* card information to QPS it was satisfied on reasonable grounds that it was necessary for a law enforcement function; and
- QPS was satisfied on reasonable grounds that the requested *go* card information was necessary for a legitimate purpose.

The OIC adopted the following approach to the review:

- identified the relevant IP Act requirements.
- gathered information through conversations with staff of TransLink, QPS and TransLink's service providers Cubic and Serco and review of documentation and websites, including relevant policies, procedures and contracts.
- assessed each QPS request for *go* card information and TransLink response to determine if the IP Act requirements were met.
- identified any general privacy issues of a systemic nature as set out in the Terms of Reference.

Where appropriate, issues were discussed with TransLink and QPS, to check the findings, canvass solutions and seek agreement on how these issues could be resolved.

## 7 Timeline of the review

Date	Action
6 August 2010	TransLink provided OIC with details of 47 matters where <i>go card</i> information had been requested, and a set of draft policies and procedures within 5 business days as requested in the Terms of Reference.
16 August 2010 onwards	OIC worked with TransLink to: <ul style="list-style-type: none"> <li>• obtain further documentation for review;</li> <li>• interview officers of TransLink and TransLink's service providers; and</li> <li>• review a further seven matters where QPS had requested <i>go card</i> information from TransLink after the review had commenced.</li> </ul>
1 September 2010	QPS provided OIC with a spreadsheet summary of requests for <i>go card</i> information.
4 September 2010	OIC attended at QPS to discuss the information contained in the spreadsheet and view details of the files in hard copy and in QPS database, QPrime.
7 September 2010	QPS provided OIC with a form drafted by the State Crime Operations Command for QPS to use when requesting personal information from TransLink.
25 and 26 October 2010	QPS forwarded information from QPS records about seven matters where QPS had requested <i>go card</i> information from TransLink after the review had commenced. OIC attended at QPS the next day to view details of the files in hard copy.
8 November 2010	Draft report hand delivered to QPS and TransLink and a short briefing given to senior officers.
12 November 2010	Formal response received from TransLink.

Date	Action
18 November 2010	Formal QPS response received.
18 November 2010	Report finalised and approved by the Information Commissioner.
November 2010	Report presented to the Speaker of the Legislative Assembly.
May 2011	OIC to assess implementation of the recommendations by TransLink and QPS.

## 8 Requests for go card information

---

TransLink provides a public transport network for people to travel in South East Queensland by bus, train or ferry. The *go card* is TransLink's electronic ticket for use throughout the network. *Go cards* are a type of smartcard, resembling a plastic credit card, which contain a chip which stores information. There are a number of technical terms and concepts associated with the *go card* system which are set out in Appendix 2.

The OIC received information from TransLink and the QPS about requests which QPS had made for *go card* information. This was compared to match the requests made by QPS with the requests received by TransLink, then divided into those received before the review began (pre-review requests) and those received after (post-review requests).

Pre-review requests were managed by TransLink on a case by case basis. Post-review requests were managed according to a new procedure developed by TransLink to address privacy issues. Under this new procedure, QPS was required to complete TransLink's form to request *go card* information. Because the post-review requests were handled differently, OIC compared the new procedures to the old procedures to determine if they were more compliant with the IP Act.

The pre-review requests were on a number of occasions not handled in accordance with the IP Act; the post-review requests were generally handled in accordance with the legislative requirements.

### 8.1 Pre-review requests

QPS made 63 requests for information in relation to 53 different matters, some of which covered 138 *go cards*. Most of these requests were sent by email and were generally made by Constables or Sergeants. While not required, it was noted that a small number of requests were authorised by a second, independent officer.

QPS records indicate that 62 of these requests related to an incident recorded in QPrime, the QPS database, and that there were reasonable grounds for QPS to believe that the *go card* information was necessary for the investigation of these incidents. These incidents included both criminal offences and missing persons.

Missing persons requests generally used similar words, such as “concerns”, “grave concerns” or “very serious concerns”, and for the majority of the missing persons there were specific factors associated with the missing persons which made them vulnerable, such as a disability, an illness or their age.

For nine of these requests, the specific law enforcement purpose was not provided to TransLink, meaning TransLink was not given sufficient information to identify the incident being investigated by QPS. For two of those nine requests, TransLink asked QPS for more information; for three others, QPS had classified them as “Highly Protected”. For each of these requests, QPS records showed that the request was related to an activity logged in QPrime, with one exception. This was a QPS record of a phone call from an officer requesting CCTV footage, with no further information. TransLink has no record of this request from QPS or of any response made by TransLink.

While requests were received by many different areas of TransLink, the majority were dealt with by the Right to Information and Information Privacy Team (RTI and Privacy Team). TransLink disclosed the personal information of *go* card holders to QPS in response to 27 of these requests. However, only 11 of the 27 requests contained enough information to allow TransLink to satisfy itself that the disclosure was necessary as set out in IPP 11(1). Four of the 27 QPS requests gave inadequate reasons why the *go* card information was required. Additional concerns were raised by another 11 of these requests, for example, the amount of information sought or the length of time between the incident and the request.

More detail and a full breakdown of the pre-review requests are provided in Appendix 3.

## **8.2 Post-review requests**

There were 16 requests for information in relation to seven matters, some of which covered 13 *go* cards, received by TransLink from QPS after the beginning of the review.

All of the requests stated why the information was needed, 12 for the investigation of criminal offences and four for missing persons. Similar words to the pre-review requests were used in the post-review requests relating to missing persons. The requests were sent to TransLink by fax, 14 on the new form developed by TransLink,

and the majority were made by Constables. All of these requests specified the incident for which the *go* card information was needed and all were directed to the RTI and Privacy Unit.

In response to these requests, TransLink gave QPS transaction histories for five *go* card users and name, address, phone numbers and contact details for eight other *go* card users.

More detail and a full breakdown of the post-review requests are provided in Appendix 4.

## **9 What did the review find?**

---

### **9.1 Obligations under the IP Act**

The IP Act only allows TransLink to disclose personal information in specific circumstances as set out in IPP 11(1), such as where the agency is satisfied on reasonable grounds that the personal information:

- is required by a law enforcement agency for law enforcement purposes, as set out in IPP 11(1)(e)
- is necessary to lessen or prevent a serious risk to an individual, as set out in IPP 11(1)(c).

Out of all the requests reviewed, this review identified that TransLink gave the QPS personal information about 142 go cards in response to 40 QPS requests. This disclosure has been assessed against the requirements of IPP 11(1)(c) and (e).

### **9.2 Did the pre-review requests and responses comply with the relevant IPPs?**

It was possible to identify 55 QPS investigations from the 63 pre-review requests. These were 27 offence investigations, 19 missing persons investigations and nine unspecified investigations.

For the nine unspecified investigations, there was no information in the TransLink material describing what QPS was investigating. In four cases, the description of the investigation was so minimal that it was not clear QPS was investigating anything, for example, the request which advised that QPS was conducting “inquiries in relation to a person who is believed to have exited a train”.

Despite this information not being provided to TransLink in every instance, QPS records in relation to all but one request clearly recorded what was being investigated. The review did not find any of QPS' requests to be without a proper purpose, i.e., all requests were made in compliance with IPP 1.

In summary, QPS requests were made as part of specific investigations, but in over half of the requests relevant information about these investigations was not communicated to TransLink. As a result, when TransLink disclosed personal information to QPS in response to those requests it could not have been satisfied on

reasonable grounds that the disclosure was necessary as set out in IPP 11(1)(c) or (e).

### **9.3 Enabling TransLink to comply**

In order to disclose personal information to QPS under IPP 11(1)(c) or (e), TransLink needs enough information to be satisfied on reasonable grounds that the disclosure is necessary. TransLink can only satisfy itself if QPS gives details of the investigations for which it needs the information. If QPS does not do this, TransLink will either have to ask for more information or refuse to disclose.

QPS accepted this, but raised concerns about two specific circumstances:

- 1) Law enforcement investigations described by QPS as “highly protected” where providing detail about the investigation to TransLink could negatively affect the investigation; and
- 2) Missing persons investigations of high risk because of the vulnerabilities of the missing person where QPS wanted to protect the privacy of the vulnerable person.

Regardless of the sensitivity of the investigation, or the nature of the information involved, TransLink needs to be satisfied on reasonable grounds that the disclosure is necessary.

#### **9.3.1 Highly protected information**

It is acknowledged that some law enforcement investigations can involve “highly protected” information, the dissemination of which should be strictly limited to where there is a “need to know” or where disclosure is required under a law.

TransLink cannot be reasonably satisfied that the disclosure is necessary in the absence of qualifying information beyond QPS’ assertion that it is so. On the other hand, providing “highly protected” information generally to TransLink and/or there being a record of the information contained outside of QPS may be damaging to the investigation.

A suggested compromise for this class of information is for QPS to brief a selected person or position within TransLink on why it is necessary to their investigation that personal go card information be disclosed. If the relevant person in TransLink comes

to the conclusion that they are satisfied the disclosure is necessary, they attest to their satisfaction on the documentary record. At no time is the content of the briefing documented in TransLink records.

If QPS and TransLink decide to implement a procedure such as this, they may wish to formalise it through a protocol.

### **9.3.2 Missing persons**

Being missing is not in and of itself a criminal offence; locating a missing person is not automatically a law enforcement activity. Something more is required for an exemption under IPP 11 to apply. Generally, the absence of the person must be linked to either an offence or to a serious threat to the life, health, safety or welfare of an individual or the public.

General words such as "concerns" or "grave concerns" will not enable TransLink to be satisfied on reasonable grounds that that disclosure of the information is necessary to lessen or prevent a serious threat to an individual, particularly if those or similar words are used in every request.

QPS made 19 pre-review requests for *go card* information about missing persons; QPS records show that 16 of these missing persons were at significant risk because of their individual circumstances. These circumstances were generally of a highly personal and/or sensitive nature, and so are not specified in this report, for example, the missing person might have had a disability or medical condition which would have exposed the person to serious risk if he or she was not found, or there were valid reasons to believe the missing person would be harmed. QPS provided a compelling statistic in support of their statement that requests for *go card* information in relation to missing persons were only made in high risk circumstances: only 19 requests were made compared to receipt of over 3230 missing person reports in 2010.

While QPS may have sound reasons to believe the *go card* information is necessary to prevent a risk to the missing person, TransLink cannot disclose personal information without satisfying itself on reasonable grounds that the personal information is required. QPS was reluctant to give this information to TransLink because of its sensitive nature.

Regardless of the sensitivity of the information, QPS will have to provide some information to TransLink supporting its request, because in its absence, TransLink will be unable to satisfy itself the provision is necessary. If TransLink were to release the information without satisfying themselves that the disclosure is necessary, they would potentially be in breach of IPP 11.

IPP 11(1)(c) requires the information be reasonably necessary to lessen or prevent a serious threat to a person's wellbeing. It would not be sufficient to satisfy this condition for QPS to declare that it holds concerns for the person's well-being. Information should be provided both on the personal circumstances of the individual concerned and how those circumstances would put the individual at threat of harm.

In some instances, providing information about the individual's personal circumstances will be sufficient in itself – for example, “the individual is 10 years old” or “the individual has alcohol-induced dementia”. In other instances, providing information on the individual's personal circumstances will not be sufficient to indicate how they would be under threat. For example, the information that “the individual suffers from severe depression” may not indicate there is a serious threat to their well-being in the absence of the additional statement – “and they are a suicide risk”.

As with many privacy issues, a balance needs to be struck between there being a sufficient flow of personal information between QPS and TransLink to enable QPS to perform their functions, and protecting the privacy of the individuals concerned. While this balance will vary according to individual cases, TransLink and QPS are required to strike it on the occasion of each request regardless of the sensitivities of the information involved.

### **Recommendation One**

TransLink only disclose personal *go* card information to QPS under IPP 11(1)(c) or (e) if it has:

- a) sufficient information about QPS' investigation to satisfy itself on reasonable grounds that the disclosure is necessary, or
- b) been satisfied by QPS in another way, for example, through discussion between a QPS officer and a specified TransLink officer, who then notes on the TransLink record that they are satisfied that the information is necessary for a law enforcement activity and can be disclosed.

#### 9.4 Only personal information which is necessary

A number of pre-review requests asked for more information than was necessary for the investigation, for example a wider date range than was necessary or too broad a category of information. In one request, four dates were stated to be relevant to the investigation, but the request and the report generated for TransLink covered a six month period.<sup>7</sup> It is important that disclosure is limited to the specific personal information that is necessary for a law enforcement activity or to lessen or prevent the serious threat to the life, health, safety or welfare of an individual or public health, safety or welfare. Therefore the request must be specific as to the type of information sought and why it is necessary, to the greatest extent practicable.

#### Recommendation Two

QPS limit its requests to the specific personal *go* card information necessary for QPS' investigation. Where necessary, QPS and TransLink should work together to clarify the scope of the request to limit the disclosure to the specific information necessary.

#### 9.5 Notation if information is disclosed

IPP 11(2) states that if information is disclosed to a law enforcement agency under IPP 11(1)(e), the agency must include with the document a note of the disclosure.

TransLink does not maintain a "file" for every *go* card. However Nextfare has a notes facility which Cubic advised could be used to make the necessary notations and that this could be started as soon as TransLink required.

#### Recommendation Three

- a) TransLink ensure that when *go* card information is disclosed to a law enforcement agency a note to that effect is added to the *go* card database (the Nextfare system) as soon as practicable.
- b) TransLink add such a note to any *go* card information which has previously been disclosed within three months from the date of this report.

---

<sup>7</sup> D10/2590

## 9.6 Adopting a formal process

TransLink provided OIC with a draft document, *Managing Information Privacy*, outlining policies and procedures, which contained a draft *Queensland Police Information Request* form.

The draft TransLink form was piloted for post-review requests. As has been identified earlier in the report, post-review requests were of a higher standard. The form ensured that:

- i) QPS authorisation for each request was clear in every instance;
- ii) QPS provided a written explanation of the activity for which the information was requested in each instance;
- iii) QPS provided information, albeit incomplete in some cases, to describe the way in which the information was necessary for a law enforcement activity or to minimise a serious threat to an individual in each instance; and
- iv) the average time for the issue of a response to each request decreased from 3.3 days to .5 days.

Two of the post-review requests were repeat requests that had been made before the review commenced and had apparently gone unanswered. This suggests that a clear process, supported by a form, would also benefit QPS. The use of a form adds structure to the process, ensures record-keeping in compliance with the *Public Records Act 2001*, and can prompt both the requesting agency and the responding agency to take into account all the relevant considerations.

As a result of the pilot and discussions held during this review, QPS and TransLink have jointly settled a form for QPS to use when requesting personal go card information from TransLink. A copy of this form, the *Queensland Police Service Information Request* form, is provided at Attachment 5. OIC has reviewed this new form against the requirements of the IP Act. The form complies with the IP Act. In addition, the form helpfully includes guidance materials for QPS officers and example statements on the purpose for seeking the information. OIC endorses this form.

### Recommendation Four

TransLink and QPS use the *Queensland Police Service Information Request* form when QPS is requesting information from TransLink.

## 9.7 QPS requesting officers

The pre-review system used by QPS to make requests was insufficiently controlled. The lack of counter-signing exposed both QPS and TransLink to the risk, however small, that an officer in QPS could obtain *go* card information for an invalid purpose. The pre-review system also lacked clarity regarding the seniority required for requesting or authorising officers.

The post-review system was better controlled. Requests had to be co-signed by a supervisor however they still did not require a specific level of seniority for the requesting or authorising officer. The form now in use requires a commissioned officer's approval for requests (see Appendix 5).

### Recommendation Five

Requests for personal *go* card information should be co-signed by a more senior QPS officer to the one making the request.

## 9.8 TransLink's privacy statement

When an agency is "authorised" to perform an action under law, the agency has a discretion whether or not it will perform the action. When an agency is "required" to perform an action under law, the agency has no discretion and must perform the action. In none of the requests examined in this review was the disclosure of the *go* card information required under a law.<sup>8</sup> However, if TransLink complies with the criteria in IPPs 11(1)(c) or (e), its disclosure of the *go* card information to QPS is authorised under a law. The Privacy Statement on TransLink's website does not mention authorised disclosures but instead states that information will only be disclosed when required by a law. As TransLink's Privacy Statement does not contemplate disclosure which is authorised under a law, it is incomplete.

### Recommendation Six

TransLink should update its Privacy Statement to state that information may be disclosed where it is "authorised or required by law".

---

<sup>8</sup> If QPS had requested TransLink to provide *go* card information by way of a warrant, TransLink would then have been *required under a law* to comply with the warrant and provide the information to QPS.

## 10 How is *go* card information managed?

---

As set out in the Terms of Reference, the review also considered general personal information handling practices related to *go* card information.

### 10.1 QPS

A full review of QPS has not been undertaken but general policy issues have been noted relating to QPS' management of *go* card information received from TransLink.

The OIC notes that QPS retained *go* card information provided by TransLink in QPrime and other QPS databases. This information is accessible throughout QPS in support of law enforcement activities state wide.

The IP Act allows personal information to be used by law enforcement agencies for law enforcement activities other than the specific investigation for which it was obtained<sup>9</sup>. However it could be contrary to the IP Act if that personal information was used for any other purpose. This might be a matter for QPS to consider in terms of record keeping practices and management of information retained within QPrime.

### 10.2 TransLink

A full review of TransLink has not been undertaken but general privacy issues have been noted relating to:

1. Policies and procedures
2. Training
3. Complaint handling
4. Recordkeeping
5. Amount of personal information collected
6. Collecting personal information
7. Deregistration of *go* cards
8. Data security.

---

<sup>9</sup> IPP 10(1)(d)

### 10.2.1 Policies and Procedures

At the time of the review, TransLink did not have approved policies for handling QPS requests for go card information. During the review TransLink provided OIC with a draft document, *Managing Information Privacy*, outlining policies and procedures for the collection, storage, disclosure and use of personal information and the procedures for staff to follow if a request for personal information is received. TransLink advised OIC that the document had been drafted in May and June 2010, and was currently being piloted with QPS. TransLink advised on 12 November that they have been operating under these draft procedures since 9 August 2010.

OIC reviewed the draft policies and procedures, and found that they were generally sound and, if adopted, would promote compliance with the IP Act. Some minor amendments would improve the way these policies and procedures give effect to legislative requirements:

- include information in section 2.1 about how people could find out about CCTV video and audio recordings;
- the final dot point in Section 2.4 which deals with law enforcement activities needs to be amended to reflect current practice, as it refers to disclosure where it is “required by law” only; and
- section 3.3.1, which discusses requests from law enforcement agencies, could be more closely aligned with the wording of IPP 11(1)(e).

Most of the pre-review matters were referred to TransLink’s RTI and Privacy Unit. After the commencement of this review, TransLink adopted a business strategy for TransLink staff to be able to refer all these matters immediately to its RTI and Privacy Unit, so that QPS requests for information can be taken out of the mainstream operations and given the careful and expert consideration required. TransLink has provided additional staffing resources to the RTI and Privacy Unit to support this strategy. It is evident from the post-review requests that implementation of a clear and consistent process, with specialist expertise, for handling personal information requests has improved compliance with the IP Act for go card information.

### 10.2.2 Training

TransLink advised that Privacy Awareness Training has been conducted for all middle management and the leadership team. Some TransLink staff interviewed said that they were aware that privacy training had been conducted, but had not attended any training themselves. Extending privacy training for all TransLink staff would assist in building awareness of the privacy principles, and support staff to put into practice any TransLink policies and procedures adopting the privacy principles.

### 10.2.3 Complaint Handling

Good complaint management is part of doing business effectively. OIC's experience is that early, personal contact with a complainant, with an aim to informal resolution, often leads to a quicker and better outcome than a system which does not address the complaint early and which deals with the complainant primarily through written correspondence. TransLink's draft policy and procedures document *Managing Information Privacy* recognises the need for a coordinated response to complaints.

Current practice is that TransLink runs a complaint management system using a system called CommentLine. A web form available on TransLink's website<sup>10</sup> directs complaints about go cards to the call centre:

*If it's about **your go card account**, please call us rather than submitting the form. We need to speak to you in person due to privacy requirements.*

Complaints by telephone are handled by TransLink as follows:

- The complaint is entered into CommentLine by the operator.
- It is then stored in a data centre run by the Department of Transport and Main Roads. Database administrators have access to the data.
- Individual complaints are allocated automatically to the Customer Service Team within TransLink by the CommentLine system, depending on the complainant's selection of options to describe the complaint.
- Once allocated, a complaint may be accessed by the transport operators, Cubic or Serco agents to whom the complaint has been allocated. If this allocation is incorrect, the complaint can be rejected, in which case it goes to the Customer Service Team in TransLink to re-allocate correctly.

---

<sup>10</sup> Viewed at <https://forms.translink.com.au/feedback.php> on 24 August 2010.

The Customer Service Team in TransLink can access the system and is responsible for resolving all matters with the customers.

Two issues arise from these procedures.<sup>11</sup>

- It is not clear whether privacy complaints are referred to the RTI and Privacy Unit.
- This system raises data security questions. The Department of Transport and Main Roads (TMR) hosts and manages the CommentLine database, and so is responsible for the storage and management of the CommentLine information. The database administrators within TMR have access to the complaints information.

TransLink should consider referring all privacy complaints to the RTI and Privacy Unit, which has the specialised knowledge to deal with them. This is identified as a strategy by TransLink in the draft policy and procedure document *Managing Information Privacy*.

OIC was advised that a new complaints management system is under development, with the current working title of “CIPM”. The design and implementation of the new complaints management system is being done to take into account privacy issues. Until CIPM is operational, a Memorandum of Understanding between TMR and TransLink would assist in managing the privacy issues in the collection, storage and management of the CommentLine information.

#### **10.2.4 Record Keeping**

In the review, there were eight matters where it was not possible to identify whether or not the requested information had been sent to QPS. There were also record keeping issues around the extent of the documentation available, location of information and duplicate records. There was one matter which neither TransLink nor QPS had recorded properly.

---

<sup>11</sup> A third issue was identified that is not directly relevant to the review. CommentLine is currently configured so that anonymous complaints cannot be accepted. This is not consistent with current Queensland Government legislation and guidelines about complaints, which either explicitly require or implicitly allow anonymous complaints – s27(1) *Whistleblower Protection Act 1994*, the Crime and Misconduct Commission’s publication *Facing the facts* at 2.9, the Queensland Ombudsman’s fact sheet *Effective Complaints Management – 6:Responsiveness* at page 2, the Office of the Public Service Commissioner’s Directive *Complaints Management Systems* 13/09.

TransLink is already taking steps to improve its record keeping, by creating a central coordinating point for receipt of requests and responses. Additionally, the draft policy and procedures manual, *Managing Information Privacy*, contains an *Information Request – RELEASE* form for recording release of information. Once implemented, this policy and form should assist with maintaining a proper record of each matter.

#### **10.2.5 Amount of information collected**

IPP 1 requires agencies only to collect personal information that is for a lawful purpose, and is necessary to fulfil the purpose or directly related to fulfilling the purpose. IPP 3 requires agencies only to collect personal information that is relevant for the purpose for which it is collected.

The Nextfare database contains a number of specific fields for information, some mandatory and some discretionary. It was not immediately apparent that all of the information collected by those fields was necessary or relevant. Neither TransLink nor Cubic had documentation to explain the reasons for including each field in the Nextfare database and for collecting the information.

TransLink should consider each of the fields, particularly those which are mandatory, and assess them against the obligations in IPP 1 and IPP 3. This information should then be used to ensure that the three methods of registration—online, hardcopy form, and telephone—collect the same necessary information.

#### **10.2.6 Collecting personal information**

IPP 2 requires agencies collecting personal information to take reasonable steps to make an individual generally aware of the purpose of the collection, any law authorising or requiring the collection, and any usual practices of disclosing information from the agency to first parties, or from first parties to second parties. The OIC refers to the words used to meet these obligations as “collection notices”.

Three collection notices were identified in the course of the review: the online Privacy Statement, the statement on the hard copy registration form, and the message given to people who telephone the call centre. The hard copy form and telephone message both refer to the online Privacy Statement, so there is a reasonable level of consistency between messages.

Call centre operators are prompted with answers to Frequently Asked Questions. TransLink provided OIC with the text response to two frequently asked questions:

- “How will you use my personal details?”
- “Does the call centre have a secure system for entering my personal details?”

In both instances, the text response was appropriate, with two exceptions:

- the responses made reference to *Information Standard 42*, which was replaced by the *Information Privacy Act 2009* from 1 July 2009; and
- the responses should be reviewed in the light of any amendments to the web based collection notice arising from the review.

All of the collection notices would be improved by greater specificity. For example, instead of referring to “the TransLink Transit Authority’s requirements”, the hard copy form could refer to “registration and maintenance of the *go* card system”. Similarly, the recorded phone message could add the words “related to your call” to the end of the second sentence after “functions and activities”.

### **10.2.7 De-registration of *go* cards**

Someone who has registered their *go* card may choose to de-register it. TransLink advised that this is done by disconnecting the link between the card and the system, but the Nextfare system retains the *go* card holder’s personal details, for example his or her name and address. Because the link has been disconnected the *go* card holder’s details are no longer connected to travel or product information, but these two sets of information could be reconnected by a database administrator. TransLink should consider making this clear to anyone who de-registers their *go* card.

### **10.2.8 Data security**

IPP 4 requires agencies to ensure that personal information is protected against loss, unauthorised access, use, modification or disclosure and against misuse.

The *go* card information is managed by Cubic, which is required to maintain computer security according to clauses in its contract with TransLink, and captured in Cubic’s Nextfare system. Access to Nextfare is available to staff of Cubic, Serco operators and two people working in TransLink’s Customer Service Team.

- OIC was advised in the course of the review that other staff of TransLink might be aware of the Customer Service Team's ability to access Nextfare, and might have been "borrowing" access to the Nextfare system on an informal basis.
- Go card information is available to retailers, although TransLink seemed to expect that retailers would not access the information unnecessarily.
- If a go card holder registers his or her go card through a retailer, they complete a hard copy form which is then handed to the retailer. The retailer either keys the details from the form into the Nextfare database, or they forward the form to Cubic to key in the details.

The form itself and the access to the system present data security issues. In particular, Cubic advised that they do not always receive the hard copy form. If the retailer keyed the data straight into Nextfare and kept the form, then the form containing the go card holder's personal information might be dealt with by the retail outlet in a way which was not secure.

In these cases, the data security seems reliant on an informal understanding rather than physical, policy or technical controls. The level of data security could be improved, to ensure that any access to go card data is in accordance with business directions and the IP Act requirements.

### Recommendation Seven

TransLink and QPS should ensure clear policies, systems and procedures are implemented to raise awareness of, and require compliance with, personal information handling practices to meet requirements of the IP Act. This includes the following:

- a) TransLink's draft policies and procedures document *Managing Information Privacy* is formalised;
- b) a clear and consistent process for managing TransLink's privacy matters is put in place;
- c) all the personal information collected for go cards is necessary, relevant and consistent across the registration methods; and
- d) TransLink establish a high level of data security in systems for accessing Nextfare, processing hard copy registration forms, and managing complaints.

# APPENDICES



## ***Appendix 1 – Terms of Reference***

---

### **Terms of Reference – Review of handling of personal information contained in go cards – August 2010**

#### **1 Objectives of the Review**

- 1.1 This review has been initiated in order to ensure that there are proper safeguards for the handling of personal information contained in go cards.
- 1.2 In particular, the review seeks to establish that:
  - 1.2.1 TransLink is satisfied on reasonable grounds that disclosure of the go card information to the Queensland Police Service is necessary on each occasion and is necessary for a law enforcement function;
  - 1.2.2 the Queensland Police Service is satisfied on reasonable grounds that the go card information is necessary on each occasion for a purpose as per the *Information Privacy Act 2009*.
- 1.3 It is hoped that the review will promote public sector and community understanding of the privacy principles, and public sector compliance with the privacy principles.

#### **2 Scope of the Review**

- 2.1 Following public interest in the use of go card information by the Queensland Police Service, the Information Commissioner has initiated a review under section 135 of the *Information Privacy Act 2009* of personal information handling practices relating to go card information.
- 2.2 The review will assess the personal information handling practices of TransLink and the Queensland Police Service against the requirements of the Information Privacy Principles and Chapter 2 of the *Information Privacy Act 2009*.
- 2.3 The review will cover TransLink and the Queensland Police Service's policies, procedures and practices, including:-
  - 2.3.1 Agency governance, including the responsibility for developing, implementing and monitoring the information management systems for the go card and access to go card information;
  - 2.3.2 Compliance with legislatively based requirements for the adoption of privacy principles and Chapter 2 of the *Information Privacy Act 2009*; and
  - 2.3.3 Compliance with Part 4 of the *Information Privacy Act 2009*, relating to the compliance of service providers with the information privacy principles.

- 2.4 This review may identify particular grounds for the issue of a compliance notice under section 158 of the *Information Privacy Act 2009*.
- 2.5 The scope of the review specifically excludes:
- 2.5.1 Queensland Police Service policies, procedures and practices with respect to obtaining information from federal agencies, for example, the Australian Tax Office, Australia Post, telecommunications carriers, or other public service registers;
  - 2.5.2 Queensland Police Service policies, procedures and practices with respect to obtaining information from other State agencies, for example, the Registrar of Births, Deaths and Marriages, the Residential Tenancies Authority, Transport and Main Roads or other public service registers; and
  - 2.5.3 Consideration of Queensland Police Service policies, procedures and practices against operational criteria.

### **3 Suitability Criteria for Assessing Performance**

- 3.1 The review will be based on an assessment of the performance of the two agencies against the requirements of the *Information Privacy Act 2009*, and any subordinate guidelines or instruments made pursuant to the legislation.
- 3.2 Where the legislation states that the agency must meet a particular requirement, that requirement is considered to be an auditable element of the legislation. The review will test whether or not the agency has complied with that requirement.
- 3.3 Where the legislation indicates that the agency should adopt a particular approach, the review will make a qualitative assessment of the extent to which the agency has adopted that approach.

### **4 Assessment Process**

- 4.1 The review will be managed by the Manager, Performance Monitoring and Reporting (Ms Karen McLeod) and the Senior Performance, Monitoring & Reporting Officer (Mr Dean Girvan).
- 4.2 A testing program will be developed to ensure that each relevant area of practice has been considered and appropriate evidence gathered to support findings. Appropriate evidence may be gathered through the following process:
- 4.2.1 Discussions with relevant staff and management;
  - 4.2.2 Observation and walkthrough of personal information handling practices;
  - 4.2.3 Examination of agency website;
  - 4.2.4 Examination of agency intranet;

- 4.2.5 Review of statistical records/reporting;
- 4.2.6 A review of policies, procedures and records of interaction between the agencies in the process of dealing with access to go card information;
- 4.2.7 A review of policies, procedures and practices for managing the go card information; and
- 4.2.8 Substantive testing of the matters where information has been requested from TransLink by the Queensland Police Service.

## **5 Reporting**

A public report will be prepared, for the Speaker of the Queensland Parliament, in accordance with section 135 of the *Information Privacy Act 2009*.

## **6 Audit Team**

- 6.1 Karen McLeod, Manager, Performance, Monitoring & Reporting and Dean Girvan, Senior Performance, Monitoring & Reporting Officer will be undertaking the review. The review will be overseen by the Acting First Assistant Commissioner, Ben Dalton.
- 6.2 A privacy officer of the Office of the Information Commissioner will assist as needed.

## **7 Administrative Matters**

### **7.1 Timing**

At this stage, it is envisaged that on-site reviews will commence in early August and will be finalised and reported on as soon as practicable.

### **7.2 Administration**

It would be greatly appreciated if a work space and access to a computer and photocopying facilities could be provided as needed for on-site visits.

### **7.3 Request for Information**

It would be greatly appreciated if you could forward the documentation listed below within 5 business days.

1. Documents describing policies and procedures for compliance with the Privacy Principles.
2. Documents describing the policies and procedures for obtaining access to go card information.

3. Any documents, (as defined in the *Public Records Act 2002*), detailing any and all interaction between TransLink and the Queensland Police Service regarding access to and use of *go* card information, at the policy or procedural level, or with respect to cases or particular matters.

If necessary, the documentation listed below might also be sought.

4. Information about the appointment of the Information Champion, and documentation about the information governance body required under the Queensland Government Enterprise Architecture guidelines.
5. The agency's policies and procedures for Information Privacy.
6. Documents relating to the Information Asset Register (as per Information Standard 44) and a copy of or link to the Information Asset Register.
7. Organisational delegations of authority relating to Information Privacy.
8. A copy of training records for agency staff attending Information Privacy training.
9. Training materials on Information Privacy courses.
10. Documentation of complaint handling systems relating to Information Privacy.
11. A copy of all statistics collated and recorded for Information Privacy purposes, including those required by Ministerial Guidelines and annually reported to the lead agency.
12. Any sections in general policy and procedures manuals dealing with privacy issues, for example, in a Code of Conduct, in the Queensland Police Service's Operational Procedures Manual or any other document.

## Appendix 2 – Glossary

Acronym or word	Definition and Brief Explanation
CommentLine	CommentLine is TransLink’s complaints management system, operated by Serco and through TransLink’s website, with data stored by the Department of Transport and Main Roads.
Cubic	Cubic Transportation Systems is an international company, listed on the New York Stock Exchange, with headquarters in California. Under contract to TransLink, Cubic designed and delivered the <i>go</i> card system, which was launched in 2008. Cubic now provides support services, including managing the <i>go</i> card information database (Nextfare).
D09/1234	This is the format of the TransLink reference number used to identify each request for <i>go</i> card information. This enables each matter to be referenced, without naming any of the people involved.
Data penetration test	A penetration test, occasionally pentest, is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. Any security issues that are found will be presented to the system owner, together with an assessment of their impact, and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. <sup>12</sup>
device	The <i>go</i> card reader is also called a “device”.
DSA	Distribution Services Agreement between Cubic and retail outlets.
go card	A <i>go</i> card is a plastic card, which resembles a credit card in appearance. It is part of an electronic smartcard ticketing system developed by Cubic Corporation and currently used on the TransLink public transport network in South East Queensland. Each <i>go</i> card stores information, including a

<sup>12</sup> From Wikipedia [http://en.wikipedia.org/wiki/Penetration\\_test](http://en.wikipedia.org/wiki/Penetration_test) viewed on 21 September 2010

Acronym or word	Definition and Brief Explanation
	credit balance that can pay for travel fares on bus, rail or ferry in South East Queensland. To use the <i>go</i> card, users "touch on" before starting a journey, and must do the same to "touch off" the service at the end of the journey. The cost of each journey is deducted from the <i>go</i> card balance. <sup>13</sup>
IP	Information Privacy
IP Act	<i>Information Privacy Act 2009</i>
IPP	Information Privacy Principle – All agencies except Queensland Health must comply with the 11 Information Privacy Principles set out in Schedule 3 of the <i>Information Privacy Act 2009</i> .
Nextfare	<p>Cubic's website describes Nextfare as follows:</p> <p>"Nextfare® is Cubic's open software and hardware platform for today's revenue management systems. Nextfare integrates a business management system and passenger devices for smart card issuing, processing and validating. The open design enables multiple agencies in a region to share resources while keeping all proprietary information separate and secure, giving agencies a way to reduce costs."<sup>14</sup></p> <p>Nextfare stores <i>go</i> card information, including the personal information collected when <i>go</i> cards are registered. In South East Queensland, Nextfare is managed entirely by Cubic.</p>
OIC	Office of the Information Commissioner
OIC	The Performance Monitoring and Reporting Team in the Office of the Information Commissioner
QPrime	Queensland Police Service (QPS) database containing information about reported occurrences, including the names and details of people involved in the occurrences, activities undertaken to investigate occurrences, lists of items involved in the occurrences, for example, stolen

<sup>13</sup> From Wikipedia [http://en.wikipedia.org/wiki/Go\\_card](http://en.wikipedia.org/wiki/Go_card) viewed on 13 August 2010.

<sup>14</sup> From Cubic's website at <http://cts.cubic.com> viewed on 20 August 2010.

Acronym or word	Definition and Brief Explanation
	property, and the results of QPS activities.
RTI	Right to Information
RTI Act	<i>Right to Information Act 2009</i>
RTI and Privacy Team	TransLink's internal business unit dealing with Right to Information and Information Privacy matters. Currently, it is managed by the Document and Records Manager.
Serco	<p>Serco is an international company headquartered in the United Kingdom and listed on the London Stock Exchange. It provides public services, including management of hospitals, prisons and educational facilities.</p> <p>Serco's website states:-</p> <p>"On behalf of our customer Queensland Transport, Serco has managed Brisbane's TransLink Call Centre (formerly TransInfo) since 1995, handling more than two million calls per annum."<sup>15</sup></p>
smartcard	A smartcard is a credit card sized card made of plastic with a microprocessor and integrated circuits built into the card itself, in addition to memory. The <i>go</i> card is a type of smartcard.
TransLink	TransLink Transit Authority, which provides mass transit for people in South East Queensland.
Third Party Network	Cubic's term to describe the network of retail outlets which provide <i>go</i> card services, for example, sell <i>go</i> cards, register <i>go</i> cards, or top up <i>go</i> card balances.

---

<sup>15</sup> From Serco's website at [http://www.serco-ap.com.au/transport/translink\\_transport\\_information\\_services.html](http://www.serco-ap.com.au/transport/translink_transport_information_services.html) viewed on 20 August 2010.



## **Appendix 3 – Detail and breakdown of pre-review requests**

### Profile of pre-review requests

There were 63 discrete pre-review requests for information, recorded on 53 matters, relating to 138 *go* cards.

Two of the requests were large multiple *go* card requests:

- one matter related to 28 *go* cards, and in this case the name, address and phone number of people with registered *go* cards was provided to QPS;<sup>16</sup> and
- one matter related to 76 *go* cards, and the names, addresses and phone numbers of 76 people with registered *go* cards was provided to QPS.<sup>17</sup>

Each of the two large requests (for information about 28 and 76 *go* cards) has been treated as one discrete request, for efficiency and because the *go* card information on each request was dealt with in the same way.

The breakdown of the types of the 138 *go* cards that were the subject of QPS pre-review requests is described in Table 1.

**Table 1 - Types of *go* cards the subject of pre-review requests**

Type of <i>go</i> card	Number
Registered <i>go</i> cards	121
Unregistered <i>go</i> cards	10
Unknown	7
<b>TOTAL</b>	<b>138</b>

<sup>16</sup> D10/20985

<sup>17</sup> D10/21069. The TransLink documentation was inconclusive as to whether or not this information was sent to QPS, but QPS confirmed that they had received the report.

TransLink disclosed *go* card information to QPS in response to 27 requests, as described in Table 2.

**Table 2 – Number of disclosures in response to requests**

<b>Number of disclosures by request</b>		
<b>Factors</b>	<b>No. of</b>	<b>%</b>
	<b>requests</b>	
TransLink disclosed personal <i>go</i> card information to QPS	27	43%
QPS records show that the requested information was not received	4	6%
TransLink did not hold the information that was requested by the QPS	15	24%
Other - for example, duplicate records, non QPS matters etc	17	27%
<b>Total number of requests</b>	<b>63</b>	<b>100%</b>

Nature of *go* card information released

Table 3 details the response for each of the 63 requests for information, and describes how this relates to the 138 *go* cards.

Information from the *go* card database (Nextfare) was generated with respect to 27 requests from QPS (out of the 63 pre-review requests) covering 129 of the 138 *go* cards (including *go* cards which might or might not have been registered).

The remaining 36 requests (out of the 63 pre-review requests) did not result in the release of *go* card information to QPS. These requests included requests for general information about the *go* card system, duplicate requests, a request from an agency other than QPS, and requests that mentioned *go* cards but which were not requests for *go* card information.

**Table 3 – Number of disclosures in response to requests**

<b>Go card information released</b>		
	<b>Requests</b>	<b>go cards</b>
Full transaction history released to QPS	14	14
Some <i>go</i> card information released to QPS	13	115
<b>Requests where <i>go</i> card information released to QPS</b>	<b>27</b>	<b>129</b>
Search on <i>go</i> card number found no registration	2	2
No records were available e.g. no <i>go</i> card in a name	14	
Response not recorded by TransLink	8	2
Not a personal <i>go</i> card request by the QPS	7	
Decision by TransLink not to respond	2	3
QPS request not located in TransLink's records	1	
<i>Go</i> card report generated for another agency	1	1
<i>Go</i> card details provided by QPS to locate devices	1	1
<b>Requests where <i>go</i> card information not released to QPS</b>	<b>36</b>	<b>9</b>
<b>TOTAL</b>	<b>63</b>	<b>138</b>

When information was provided to QPS, the information was either a report from the Nextfare database detailing the transaction history for a *go* card, or a report providing some *go* card information, for example, the name and address of the *go* card holder.

14 requests involved transaction histories (for 14 *go* cards), which detailed the time, date and location of travel tags on or off a bus, train or ferry and the impact of each journey on each *go* card's credit balance. The average time period covered by the transaction histories was 107 days. Six of the transaction histories were for periods greater than 3 months.

Table 3 shows that the 13 requests resulted in the provision of some *go* card information to QPS about 115 *go* cards. The breakdown of this information was:

- the name, address and/or telephone contact details only for registered *go* card holders (7 requests for 109 *go* cards);
- *go* card numbers and information about tags (5 requests for 5 *go* cards); or
- the status and expiry date of a *go* card for use in court (1 request for 1 *go* card).

Out of 138 *go* cards involved in the pre-review requests, TransLink gave full transaction histories to QPS for 14 *go* cards and some information for 115 *go* cards. The remaining nine *go* cards that were the subject of requests did not result in information about the *go* card being passed from TransLink to QPS.

#### Response time

The average response time for TransLink to respond to a request for *go* card information was 3.3 days.

The pattern of response times is described in Table 4.

**Table 4 – Pattern of TransLink’s response times to requests**

<b>Response Time</b>	<b>No.</b>	<b>%</b>
Same day	20	32%
One day	12	19%
Two days to a week	16	25%
Eight days to a fortnight	3	5%
Twenty days or more	3	5%
No response	9	14%
<b>TOTAL</b>	<b>63</b>	<b>100%</b>

### Methods of communication

The preferred method of communication between QPS and TransLink for requests and responses was email, which accounted for around 60% of all requests and responses. Table 5 depicts the communication methods for pre-review requests.

**Table 5 – Communication methods for requesting and releasing go card information for pre-review requests**

Method of request		Method of release	
8 Telephone	13%	2 Telephone	3%
14 Fax	22%	6 Fax	10%
37 Email	59%	39 Email	62%
2 Letter	3%	0 Letter	0%
2 Other	3%	3 Other	5%
		<b>Other outcomes</b>	
		3 Duplicate Records	5%
		8 Response not recorded	13%
		2 Decision not to respond	3%
<b>63 Total Requests</b>	<b>100%</b>	<b>63 Total Responses</b>	<b>100%</b>

Note - Numbers may not add up due to rounding

### Who dealt with requests

Pre-review requests came from QPS into multiple entry points within TransLink, and responses were primarily made by the Right to Information and Information Privacy Team (RTI and Privacy Unit) within TransLink, as shown in Table 6.

**Table 6 - Comparison of contact points for receipt of and response to requests**

Contact point for request		Exit point for release	
13 TransLink	21%	1 TransLink	2%
32 TransLink RTI and Privacy Unit	51%	46 TransLink RTI and Privacy Unit	73%
10 Cubic	16%	0 Cubic	0%
6 Serco	10%	0 Serco	0%
2 Other	3%	3 Other - in person	5%
		<b>Other outcomes</b>	
		3 Duplicate Records	5%
		8 Response not recorded	13%
		2 Decision not to respond	3%
<b>63 Total Requests</b>	<b>100%</b>	<b>63 Total Responses</b>	<b>100%</b>

Note - Numbers may not add up due to rounding

## Types of QPS investigations

TransLink records enabled identification of the nature of QPS investigation of a criminal matter for 43% of the pre-review requests for go card information. These were split relatively evenly between offences against the person and offences against property. Table 7 provides the details of the reasons for the requests.

**Table 7 – Reasons for requesting information for pre-review requests**

<b>TransLink records of QPS requests for personal go card information</b>			
<b>Activities</b>		<b>Details of activities</b>	
27 QPS investigations	43%	<b>Details of QPS investigations:</b>	<b>%</b>
		15 homicide, assault, sexual offences	56%
		12 burglary, theft, possession	44%
19 missing persons	30%		
9 unspecified investigation	14%	<b>QPS records for unspecified investigations:</b>	
		1 unspecified (phone call about CCTV)	11%
		5 involving offences against the person	56%
		2 involving offences against property	22%
		1 which QPS considered a duplicate	11%
<b>55 QPS investigations</b>			
8 other	13%	<b>Not seeking go card information for QPS:</b>	
		1 internal legal advice	13%
		3 advice on process	38%
		1 authorised by migration law	13%
		3 Duplicate	38%
<b>63 Total Requests</b>	<b>100%</b>		

Note - Numbers may not add up due to rounding

From TransLink's perspective, nine of QPS requests related to unspecified investigations, that is, the information provided by QPS was insufficient to identify what type of matter was being investigated. From QPS' perspective, there was only one investigation which was unspecified. The reasons for this difference are discussed further in the next chapter.

Examples of the information provided by QPS to TransLink in the unspecified investigations included the following descriptions:

- "I am contacting you in an effort to obtain GoCard transaction histories which are required for a current police investigation."<sup>18</sup>

<sup>18</sup> D10/2832

- A call centre operator reported “I have had a request from Constable (name) for the transaction history for goCard (number) for a case he is working on.”<sup>19</sup>
- “I am currently making inquiries in relation to a person who is believed to have exited a train ...”<sup>20</sup> After a follow up call from TransLink to obtain more information as to the reason for the request, the file noted the officer’s response that it was “...a public safety issue.”<sup>21</sup>
- A phone call from a person stating he was from QPS, seeking information urgently as he had “a man in custody now” and thought the man’s go card might be stolen.<sup>22</sup>
- “As part of ongoing police investigations, the GoCard transaction details for the below listed persons is requested.”<sup>23</sup>

There were two occasions where TransLink contacted QPS to obtain more information about the request, before deciding whether or not to provide the information.<sup>24</sup>

For three of the unspecified investigations, QPS information about the investigation was of a highly sensitive nature, described in QPS records as being “Highly Protected”.

#### Authorisation for making the request

According to TransLink records, QPS pre-review requests were generally made by Constables (60% of requests) or Sergeants (27% of requests). In only one instance was a request made by a commissioned officer. QPS records indicate that most requests were made by Constables (79% of requests). This is detailed in Table 8.

In the TransLink record, there were five cases in which the original request was authorised by an independent second person, whereas QPS record indicates this occurred for nine requests.

Scrutiny of QPS and TransLink records identified a number of reasons for the differences between the TransLink and QPS records. The most common reason for the difference was QPS record specifying a requesting officer and an authorising

<sup>19</sup> D10/10379, identifying details have been removed.

<sup>20</sup> D10/21069

<sup>21</sup> D10/21069

<sup>22</sup> D09/33443

<sup>23</sup> D10/1420

<sup>24</sup> D10/21069 and D09/32509

officer, where the TransLink record showed only the authorising officer (seven requests).

**Table 8 – Requesting QPS officers**

Requesting QPS Officers - from TransLink record		Requesting QPS Officers - from QPS record	
38 Constable	60%	50 Constable	79%
17 Sergeant	27%	11 Sergeant	17%
1 Officer in Charge	2%	1 Administrative Officer	2%
5 unknown	8%	0 unknown	0%
2 n/a	3%	1 n/a	2%
<b>63 TOTAL</b>	<b>100%</b>	<b>63 TOTAL</b>	<b>100%</b>
Authorised by a second QPS person	5	Authorised by a second QPS person	9

For the purposes of the review, a rank with the word “Constable” in the title was treated as a Constable, and a rank with the word “Sergeant” in the title was treated as a Sergeant. QPS confirmed that this was a reasonable approach, and advised that an administrative position at the public service classification level of AO4 was equivalent to a Sergeant.

#### QPS activities when requesting personal information

QPS records of the requests were examined to identify the ways in which QPS might have satisfied itself on reasonable grounds that the request was necessary for an activity related to the enforcement of laws.<sup>25</sup> Factors that were considered to be indicators of QPS’ compliance with the IP Act were whether or not there was a record of the law enforcement activity (for example, an occurrence logged in QPS database, QPrime), whether or not QPS record incorporated a documented reason for the request and whether or not the request was authorised.

Table 9 details the extent to which these factors could be identified for each request.

QPS records showed that each request was related to an activity logged in QPrime, with one exception. This was a QPS record of a phone call from an officer requesting CCTV footage, with no further information. TransLink has no record of this request from QPS or of any response made by TransLink. According to QPS records, each QPS request had a documented reason with apparent validity, with the

<sup>25</sup> As per Section 29 IP Act and the information privacy principles

one exception being the same matter already noted. For the purposes of the review, this one matter which was not logged in QPrime or documented has been treated as a one off exception. Otherwise, QPS records indicate that QPS had a good reason for requesting the go card information on each occasion.

**Table 9 –Personal information and QPS activities**

<b>Factors indicating QPS compliance with IP Act</b>						
<b>Factors</b>	<b>Yes</b>		<b>No</b>		<b>Other*</b>	
	<b>No. of</b>	<b>%</b>	<b>No. of</b>	<b>%</b>	<b>No. of</b>	<b>%</b>
	<b>requests</b>		<b>requests</b>		<b>requests</b>	
Logged in QPrime and given a number	46	73%	1	2%	16	25%
With a documented reason	47	75%	1	2%	15	24%
Where the reason had validity on its face	63	100%	0	0%	0	0%
Authorised by a sergeant rank or higher	20	32%	40	63%	3	5%
The QPS record documented how the information was actually used	28	44%	0	0%	35	56%
Where there was no risk of secondary usage	40	63%	23	37%	0	0%
<b>* Other includes duplicates, non QPS matters etc</b>					<b>Total No. of requests 63</b>	

Note - Numbers may not add up due to rounding

Analysis of the factors listed in Table 9 identified two areas of possible concern for QPS:

- the level of authorisation for making the request for information, which on QPS records was not authorised by a more senior officer for 40 out of 63 requests (70%); and
- the prospect that the go card information was stored in such a way that it could be retrieved and re-used improperly for another purpose, which was the case for 23 out of 63 requests (37%).

#### Factors for assessing disclosure of go card information

An examination was made of the TransLink records for the 27 instances where TransLink disclosed go card information to QPS, to identify how TransLink might

have satisfied itself on reasonable grounds that the disclosure of the information was necessary for a purpose described in the IP Act.

Factors that were considered to be indicators of TransLink's compliance with the IP Act were whether or not there was a documented reason for the request, whether or not the grounds given for the disclosure were reasonable on their face, and whether or not the reason fell within the reasons described in the IP Act. Table 10 provides the details of this analysis.

**Table 10 – Appropriate disclosure of information**

<b>Factors for assessing TransLink's disclosure of information to QPS</b>					
<b>Factors</b>	<b>Yes</b>		<b>No</b>		<b>Total</b>
	<b>No. of</b>	<b>%</b>	<b>No. of</b>	<b>%</b>	<b>No. of</b>
	<b>requests</b>		<b>requests</b>		<b>disclosures</b>
A reason was given for the request	23	85%	4	15%	27 / 100%
The reason was given in writing	19	70%	8	30%	27 / 100%
The reason did not raise further questions	16	59%	11	41%	27 / 100%
The reason could be linked to the IP Act	21	78%	6	22%	27 / 100%
<b>Requests which met all of the requirements i.e. gave a reasonable written reason linked to the requirements of the <i>Information Privacy Act 2009</i></b>	<b>11</b>	<b>41%</b>	<b>16</b>	<b>59%</b>	<b>27 / 100%</b>

11 out of 27 (approximately 41%) of disclosures satisfied all of the above indicators that the disclosure of go card information from TransLink to QPS was in accordance with the IP Act.

TransLink disclosed go card information in response to four requests where no reason was given for the request. These were a phone call for information relating to a missing person investigation,<sup>26</sup> a matter linked to an earlier request,<sup>27</sup> and two requests for information about two go cards on one matter.<sup>28</sup>

There were 11 disclosures of information in response to requests from QPS which, on their face, raised further questions. Leaving aside the requests already described

<sup>26</sup> No TransLink reference number

<sup>27</sup> D10/20985

<sup>28</sup> D10/10379

for which no information was provided, examples of the issues raised by these requests were:

- a request where information was sought for a six month period, although the investigation was concerned with four specific days,<sup>29</sup>
- on a missing person request, a lapse of seven months between the date that the person went missing and the date of the report to QPS and request to TransLink;<sup>30</sup>
- three missing person requests on one matter with no dates provided as to when the persons went missing,<sup>31</sup> and
- information sought about males and females for a matter where QPS stated they were tracking information about a male.<sup>32</sup>

In response to each of these requests, more specific or detailed information would have assisted TransLink to identify exactly what information was necessary for the QPS activity.

#### Missing persons

19 of the 63 pre-review requests related to investigations of missing persons. QPS adopted a fairly standardised form of words in their requests for information about missing persons to try to establish a link to a law enforcement activity or a threat to the life, health, safety or welfare of the individual. For example, the following words were used:

- “Concerns are held for the safety and welfare of the missing person as his mother reports that his failure to return home is out of character.”<sup>33</sup>
- “VERY SERIOUS CONCERNS are held for the safety of the missing person due to the circumstances of her disappearance.”<sup>34</sup>
- “Grave concerns are held for her safety as she has not been sighted by her parents from Sept 2009.” (Note – 230 days, or approximately seven months, had elapsed between the disappearance and the date of QPS request.

---

<sup>29</sup> D10/2590

<sup>30</sup> D10/8419

<sup>31</sup> D10/1499

<sup>32</sup> D10/21069

<sup>33</sup> D10/3265

<sup>34</sup> D10/1485

Excluding this matter, the average time identifiable between the disappearance and the request was seven days.)<sup>35</sup>

- “Concerns are held for her health and safety as this is out of character for the Missing Person. This matter is being treated as a criminal investigation.”<sup>36</sup>
- “Grave concerns are held due to this out of character disappearance. This matter is being treated as a criminal investigation.”<sup>37</sup>
- “Grave concerns are held for her safety.”<sup>38</sup>
- “... concerns are held for his welfare.”<sup>39</sup>
- “Concerns are held for the safety and welfare of the missing person as his carers report that his failure to return home is out of character.”<sup>40</sup>

In two cases the police added “This information is required in the interests of justice.”<sup>41</sup>

Inspection of QPS files identified that there were issues of particular concern for 16 out of 19 missing person requests that had not been communicated to TransLink. QPS records characterised these 16 instances as high risk, as a result of a risk assessment conducted by the Missing Persons Unit. Risk factors were associated with personal vulnerability, for example, if the missing person was a juvenile (seven requests), had a disability or illness (four requests), or the circumstances of their disappearance raised the possibility that the missing person was at risk of harm (five requests). Five of the seven juveniles had these types of additional risk factors associated with their disappearance.

QPS considered that the risk assessment narrowed the number of requests for information appropriately. QPS advised that over 3230 reports of missing persons had been received by the Missing Persons Unit in the calendar year of 2010, compared to the 19 instances where QPS had contacted TransLink for *go* card information. QPS stated that it was only in high risk matters that *go* card information would be sought.

---

<sup>35</sup> D10/8419

<sup>36</sup> D10/20734, D10/36626

<sup>37</sup> D10/1379

<sup>38</sup> D09/33362

<sup>39</sup> D09/35714

<sup>40</sup> D10/1552

<sup>41</sup> D10/20734, D10/1379

There were three requests which were an exception to this general rule about risk assessment. These requests were handled through a regional office, and were not processed through the Missing Persons Unit, so the reports of missing persons did not go through the risk assessment process.<sup>42</sup>

QPS confirmed that they had not provided full details about their reasons for seeking go card information to TransLink, out of privacy concerns around revealing the personal information of the missing persons to TransLink.

TransLink was not able to provide QPS with the information requested for 14 of the 19 missing persons requests. For 13 of these requests, QPS provided TransLink with the name of the missing person to see if there was a registered go card in that name, and TransLink advised that there was no registered go card in the name of the missing person. One request was for information about a long distance bus journey, which was not contained in the go card system.<sup>43</sup>

Where TransLink did provide information to QPS, the information was not of assistance to QPS' investigation. In response to two requests, TransLink provided information which pre-dated the disappearance of the missing person, and was not required for the investigation.<sup>44</sup> For one request, the information was for a person of the same name but a different date of birth,<sup>45</sup> and for two requests, the information was not relevant to the period in question.<sup>46</sup> In all five of these cases, the missing persons were located by means other than by using the TransLink information.

---

<sup>42</sup> D10/1499 – three requests

<sup>43</sup> D10/9115

<sup>44</sup> D10/18069 – two requests

<sup>45</sup> D10/8419

<sup>46</sup> D10/1499 – two requests



## **Appendix 4 – Detail and breakdown of post-review requests**

TransLink gave OIC details of seven matters containing requests from QPS made after the review commenced (post-review requests)<sup>47</sup>. These seven matters contained 16 requests for information, relating to 13 registered go cards.

In response to the 16 QPS post-review requests, TransLink generated and gave to QPS five go card transaction histories from the Nextfare database, and eight reports providing name, address and phone number contact details for each of the go cards. In three cases, go card records were not available.

In contrast to the pre-review requests which were made largely by email (58%), all of the 16 QPS post-review requests came by fax, and 14 of the 16 requests were made using the new form. All went straight to the TransLink RTI and Privacy Unit.

In 14 cases, TransLink responded by email, in one case by fax and in one case in person. The average response time was 0.5 days.

The reasons for requesting the information for post-review requests are summarised in Table 11. There were no unspecified investigations in the post-review requests.

**Table 11 – Reasons for requesting information for post-review requests**

<b>Nature of activity</b>		<b>Details of QPS investigations</b>	
11 QPS specified law enforcement	69%	10 homicide, assault, sexual offences	63%
		1 burglary, theft, possession	6%
0 QPS unspecified investigation	0%	0 unspecified investigation	0%
4 QPS described missing person	25%	4 missing persons	25%
1 Coronial matter	6%	1 Coronial matter	6%
<b>16 Total Requests</b>	<b>100%</b>	<b>16 QPS investigations</b>	<b>100%</b>

QPS requests for information about missing persons stated:

- “There are concerns for health and safety and an investigation has been started regarding her disappearance. This information is sought in accordance with the Information Privacy Act 2009 11(c) or (e). [sic]”<sup>48</sup>

<sup>47</sup> From 5 August 2010 onwards

<sup>48</sup> D10/1598

- “Grave concerns are held for her health and safety and a criminal investigation has been commenced in relation to her disappearance. Information is sought in accordance with the Information Privacy Act 2009 s 11(c) or (e). [sic]”<sup>49</sup>

The TransLink record was that QPS post-review requests were generally made by Constables (88% of requests). In two instances, requests were made by Assistant Intelligence Analysts. This is detailed in Table 12.

**Table 12 – Requesting QPS officers**

Requesting QPS Officers		Co-signed by supervisor (all sergeant or higher)	
14 Constable	88%	13	81%
0 Sergeant	0%		0%
2 Assistant Intelligence Analyst	13%	2	13%
0 unknown	0%	1	6%
0 n/a	0%		0%
<b>16 TOTAL</b>	<b>100%</b>	<b>16 TOTAL</b>	<b>100%</b>

Note - Numbers may not add up due to rounding

<sup>49</sup> No TransLink reference number – request dated 8 August 2010

## Appendix 5 – Request Form

### Queensland Police Service Information Request

Requesting officer:

		QPRIME Reference:			
Name		Rank		Registered No.	
Region		District		Station	
Email		Phone		Fax	
"I certify that this information is reasonably necessary pursuant to Principle 11 (1) of the <i>Information Privacy Act 2009</i> "					
Requesting Officer Signature			Date		

Commissioned Officer Authorisation:

Name		Rank		Registered No.	
Region		District		Station	
"I am satisfied this information is reasonably necessary pursuant to Principle 11 (1) of the <i>Information Privacy Act 2009</i> ".					
Commissioned Officer Signature			Date		

Information and Reason for request including what is being investigated.					
<ul style="list-style-type: none"> <li>• why the information is necessary for the investigation; and</li> <li>• any law requiring or authorising TransLink to provide the information.</li> </ul>					
The TransLink Transit Authority must not disclose personal information unless an exception in paragraphs (a) to (f) of the IPP 11 (1) of the <i>Information Privacy Act 2009 (Qld)</i> applies. TransLink will assess on a case by case basis whether an exception applies. TransLink may disclose information, if it is satisfied on reasonable grounds, that the disclosure of information is necessary for 1 or more of the paragraphs in IPP 11 (1) (e) (i) to (v).					
<b>Internal use only</b>					
Date request received by TransLink:	/	/	Receiving officer:		
Send to: <b>RTI &amp; Privacy Unit - GPO Box 50, Brisbane, Qld 4001 Phone: 3167 4324 Fax: 3167 4001</b>					
Email: <a href="mailto:privacy@translink.com.au">privacy@translink.com.au</a>					

### Instructions for QPS members

1. The information in the request form must be sufficient to satisfy the provisions of IPP and enable Translink to make an informed decision to release their information however the request should not compromise the operational integrity of the investigation.
  - a. For example, it is appropriate to say *'to identify witnesses for investigations into a sexual assault which occurred on a bus on the afternoon of 5 December 2009'* but inappropriate to mention intimate details of a child victim.
  - b. For example, *'break and enter investigation'* is insufficient however *'conducting enquiries to ascertain if offenders have used a go card stolen from a break and enter on 5 December 2009 at Chermside'* is appropriate.
2. For missing persons requests, *'concerns over a missing person'* is insufficient however *'concerns for the safety of a missing 10 years old child'* (refer to known vulnerabilities in Chapter 12 of the Operational Procedures Manual and the missing person risk assessment process).
3. For matters rated as 'Highly Protected', contact is to be made with the Detective Chief Superintendent, State Crime Operations Command (3364-6168) and an approach will be made to the Manager, Translink to engage in negotiations to ensure the security of the information is protected but that sufficient security protocols and processes exists for Translink to make a decision to release personal information.
4. Your request must be signed by a Commissioned Officer.
5. Fax or email page one **ONLY** of this document.
6. The provisions of *IPP 11 – Limits on disclosure* is attached for information and is the legislation Translink assess QPS requests on. Normally, the QPS rely on provisions 11(c) or 11 (e).

### 11 IPP 11—Limits on disclosure

(1) An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the **relevant entity**), other than the individual the subject of the personal information, unless—

(a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or

(b) the individual has expressly or impliedly agreed to the disclosure; or

(c) the agency is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or

(d) the disclosure is authorised or required under a law; or

(e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(f) all of the following apply—

the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;

it is not practicable to obtain the express or implied agreement of the individual before the disclosure;

(iv) the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

(2) If the agency discloses the personal information under subsection (1)(e), the agency must include with the document a note of the disclosure.



## **Appendix 6 – go card retail outlets**

There are 656 retail outlets which can assist people in different ways with their go cards, for example, buying a go card, registering a go card or topping up the go card balance.<sup>50</sup> These retail outlets include newsagents, fare machines, convenience stores, railway stations and other outlets. TransLink advised that 382 of these retail outlets provide services under an agreement with Cubic, derived from the Prime Contract between TransLink and Cubic.

TransLink provided OIC with a copy of a Distribution Service Agreement (DSA) between Cubic and a retail outlet.<sup>51</sup> This document is the second generation of contract with retail outlets, and has been entered into with retail outlets who can register go cards. The DSA contract dates vary depending on when the retailers signed up. The first DSA was signed in 2007. From 1 July 2010, this DSA is in place for all relevant retail outlets (retail outlets who can register go cards and offer refunds).

Clause 13 of this Service Agreement deals with privacy and makes reference to extracts from the Prime Contract between Cubic and TransLink (the Privacy Plan, Privacy Obligations and the Specification) captured in Appendix SP to the contract with the retailers. It is TransLink's view that by signing this contract, the retail outlets adopt the Privacy Plan.

This DSA contract is basically sound. Some issues might be worth review in future iterations. The DSA refers to the Commonwealth Privacy Principles and not the Information Privacy Principles contained in the *Information Privacy Act 2009*. The DSA also mentions an annual privacy audit, which both TransLink and Cubic advise has not taken place. Future versions of the DSA might be developed in the light of further consideration of these two issues.

The TransLink website listed 111 retail outlets which could register a go card, as summarised in Table 13.

---

<sup>50</sup> Viewed at

[http://www.translink.com.au/agents.php?action=any&cardtype=adult&region=all&suburbs%5B%5D=all&pay%5Bcash%5D=on&pay%5Bftpos%5D=on&pay%5Bcredit%5D=on&search\\_retailers=Search](http://www.translink.com.au/agents.php?action=any&cardtype=adult&region=all&suburbs%5B%5D=all&pay%5Bcash%5D=on&pay%5Bftpos%5D=on&pay%5Bcredit%5D=on&search_retailers=Search) on 2 September 2010

<sup>51</sup> Distribution Services Agreement for the Various Services Required for the Distribution of Smart Cards for an Integrated Ticketing System for South-East Queensland.

**Table 13 Retail outlets registering go cards**

<b>Retail Outlet</b>	<b>No.</b>
Railway ticket office	87
Newsagent	21
Bus interchange	1
Post office	1
Other retail	1
<b>TOTAL</b>	<b>111</b>

Cubic advised that 1547 *go* cards had been registered through a railway ticket office and 128 *go* cards had been registered through the Third Party Network, for example, newsagents. Of the *go* cards that were covered by this review, one was registered in a railway ticket office and none were registered at a retail outlet.

## **Appendix 7 – TransLink’s Online Privacy Statement**

---

Viewed at <http://www.translink.com.au/privacy.php> on 24 August 2010

### **Privacy statement**

[Home](#) > Privacy statement

The TransLink Transit Authority is committed to protecting your personal information. Our objective is to protect the privacy, accuracy and security of your personal information in accordance with the *Information Privacy Act 2009 (Qld)*.

### **Collecting information**

We will only collect personal information that is relevant and necessary for our functions and activities.

We collect and store personal information that you, our contractors or business partners provide to us.

Personal information collected by TransLink generally comprises name, address, date of birth, gender, contact details (such as phone, fax and email), certain financial information (such as credit card details or bank account details) and information relevant to concession fares (such as student or pension details).

### **Website**

When you visit our website, our server makes a record of your visit and logs the following information for statistical purposes only:

- The user's server address.
- The user's top level domain name (for example .com, .gov, .au, and so on).
- The date and time you visited the website.
- The pages accessed and documents downloaded.
- The type of browser you use.
- No attempt will be made to identify users, or their browsing activities, unless we are lawfully required to do so for an investigation or law enforcement purposes.

## Access to this website

You must not use any application, system or method to access information on this website, including information in relation to *go* card accounts, other than through ordinary use of this website by methods purposely made available on this website. You must not provide to any person, or invite or solicit any third party to provide you with, passwords or other information to enable such access.

## Emails

Your email address is recorded if you send us an email, however, we will not use your email address other than for the purpose for which you provided it. Emails in which assistance is requested will be forwarded to the relevant TransLink Transit Authority officer and/or our contactor and business partner.

Email correspondence sent to this website will be treated as a public record and will be retained in line with relevant legislation.

Email messages may be monitored by our web team for system troubleshooting and maintenance purposes.

## Smart card (including *go* card)

Our use of your personal information will depend on whether you are a 'registered' smart card holder or whether you obtain an 'unregistered' smart card.

### Unregistered smart cards

If you obtain an unregistered smart card - your details will be retained as follows:

Unregistered smart cards	Retention of personal information	Record of financial transaction	Hardcopy of financial transaction	Archive period
Cash/Debit card/Credit card	Not retained	3 Years	7 Months	5 Years

## Registered smart cards

If you choose to register your smart card, your personal information will be securely held on the central computer and linked to the serial number of your smart card. Your physical smart card will not hold any personal information.

Your personal information may be used for the following purposes:

- Allowing you to top up your smart card;
- Allowing you to obtain a replacement card;
- Allowing you to 'hotlist' or cancel a lost or stolen card to protect the stored value;
- Allowing you to access your journey history;
- Allowing us to notify you of changes to your smart card (for example impending card expiry);
- Allowing us to address any queries and complaints you may have regarding your smart card;
- Providing you with information directly related to our functions and activities; and
- Facilitating security measures to guard against fraud or inappropriate use of your card.

## Call centre

If you call the call centre, your telephone call will be recorded. This assists TransLink to carry out its functions and objectives.

If you do not want your telephone call recorded, you may tell the consultant this. If you tell the consultant that you do not want your telephone conversation recorded, you will be directed to the TransLink website or requested to mail your enquiry to TransLink in writing.

If you agree to the telephone call being recorded, all voice recordings are handled in accordance with the *Information Privacy Act 2009*.

## **CCTV and audio voice recordings**

At times, while using TransLink services, you may be video recorded by way of CCTV or conversations you have with TransLink staff and business partners may be audio recorded. TransLink makes these recordings to assist with ensuring the safety of passengers, TransLink staff and business partners and to ensure the security of the TransLink network.

All video and audio recordings are made and handled by TransLink in accordance with the *Information Privacy Act 2009* and any relevant legislation.

## **Disclosure of personal information**

In order to perform our functions and activities, we may be required to disclose your personal information to third parties, such as:

- Your bank or financial institution;
- Business partners where we outsource functions, such as information services, software development or transport planning;
- Our contracted public transport business partners, such as Queensland Rail
- Research organisations for the purpose of obtaining data about our services to assist us to improve the delivery of our functions and activities;
- Other organisations such as law enforcement agencies which we may be required to disclose information to as required by law.

## **Personal information quality**

We take reasonable steps to ensure that your personal information is stored accurately.

Please contact us if you believe the personal information we hold about you is not complete or up to date. (See contacting us below).

If we disagree with your request to correct your personal information, you may request that a statement noting your disagreement be attached to your information.

## **Personal information security**

We will protect the personal information we hold against loss, unauthorised access, use, modification and disclosure. We have a range of physical and technological procedures in place to provide a secure environment.

## Cookies

The TransLink Transit Authority website uses cookies for the journey planner. A cookie is a piece of information or small file that an internet website sends to your browser when you access information at that site. No attempt is or will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect activity logs.

## External links

The website contains links to non-TransLink Transit Authority websites. The TransLink Transit Authority is not responsible for the privacy or security practices or the content of those websites.

## Contact us

If you have any queries about our privacy and security practices, please contact:

Privacy Officer  
TransLink Transit Authority  
GPO Box 50  
Brisbane  
Queensland 4001

**Email** [privacy@translink.com.au](mailto:privacy@translink.com.au)

**Phone** 3167 4324

### National Relay Service

- TTY (teletypewriter): 13 36 77 and ask for (07) 3167 4324
- Speak and Listen (speech-to-speech relay): phone 1300 555 727 and ask for (07) 3167 4324
- Internet relay: connect to the [National Relay Service](#) and ask for (07) 3167 4324

For general information on TransLink contact our call centre on 13 12 30.