



## Office of the Information Commissioner Queensland

### **Camera surveillance and privacy**

Review of camera surveillance use by Queensland government agencies and compliance with the privacy principles in the *Information Privacy Act 2009* (Qld).

OIC thanks agencies for their cooperation throughout the review process and for the courtesy displayed towards the officers undertaking the assessment. In undertaking this review, OIC recognises the commitment of agencies handling information privacy matters and their desire for continuous improvement.



This report to the Queensland Legislative Assembly by the Office of the Information Commissioner is licensed under a Creative Commons – Attribution License. People reading or using this report may do so in accordance with the following conditions: Attribution (BY), requiring attribution to the original author.

© The State of Queensland (Office of the Information Commissioner) 2012

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: **978-0-646-58359-4**

July 2012

The Honourable Fiona Simpson MP  
Speaker of the Legislative Assembly  
Parliament House  
George Street  
BRISBANE Q 4000

Dear Madam Speaker

I am pleased to present *Camera surveillance and privacy: Review of camera surveillance use by Queensland government agencies and compliance with the privacy principles in the Information Privacy Act 2009 (Qld)*. This report is prepared under section 135 of the *Information Privacy Act 2009*.

The report reviews personal information handling practices, in particular compliance with the Information Privacy Principles, 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

<b>1</b>	<b>Executive Summary .....</b>	<b>1</b>
<b>2</b>	<b>Recommendations .....</b>	<b>2</b>
<b>3</b>	<b>Introduction .....</b>	<b>5</b>
<b>4</b>	<b>Privacy – A systemic issue.....</b>	<b>13</b>
<b>5</b>	<b>Information Privacy Principles 1 - 3 – Collection .....</b>	<b>19</b>
<b>6</b>	<b>Information Privacy Principle 4 – Data storage and security .....</b>	<b>34</b>
<b>7</b>	<b>Information Privacy Principle 5 – Individual can find footage.....</b>	<b>41</b>
<b>8</b>	<b>Information Privacy Principle 6 – Individual can access footage .....</b>	<b>45</b>
<b>9</b>	<b>Information Privacy Principle 9 – Primary use of footage .....</b>	<b>50</b>
<b>10</b>	<b>Information Privacy Principles 10 &amp; 11 – Other use and disclosure .....</b>	<b>53</b>
<b>11</b>	<b>Information Privacy Principles – Contractors.....</b>	<b>59</b>
<b>12</b>	<b>Information Privacy Principles – Overseas transfer of information .....</b>	<b>61</b>
<b>13</b>	<b>Conclusion.....</b>	<b>63</b>
	<b>APPENDICES.....</b>	<b>67</b>
	Appendix 1 – Acronyms	69
	Appendix 2 – The Information Privacy Principles	71
	Appendix 3 – Terms of Reference	79
	Appendix 4 – Office of Economic and Statistical Research Survey Report	83
	Appendix 5 – Agency Case Studies	143
	<b>1    <i>The Department of Communities</i></b>	<b>143</b>
	<b>2    <i>Ipswich City Council</i></b>	<b>149</b>
	<b>3    <i>James Cook University</i></b>	<b>155</b>
	<b>4    <i>Logan City Council</i></b>	<b>159</b>
	<b>5    <i>Townsville City Council</i></b>	<b>163</b>
	Appendix 6 – Ipswich City Council Request Form	171
	Appendix 7 – Western Downs Regional Council collection notice	173



# 1 Executive Summary

---

The use of camera surveillance systems by government agencies is substantial. In total, Queensland government agencies use more than 20,000 cameras to monitor people in public spaces. As the use of camera surveillance is significant, so too are the implications for privacy.

This review has examined the systemic practice of camera surveillance in Queensland government agencies and the extent to which camera surveillance systems were designed and operated with privacy considerations in mind.

The reviewed camera surveillance systems were generally operated in a practical way, in order to deliver public safety and security, and with respect for privacy. This could be attributed almost entirely to the experience and commitment of the operatives who set up and run the systems.

However, there were significant privacy-related gaps in the administration of the systems. One common example was the inability for individuals to discover or access footage which contained images of them. Another example was that arrangements with other agencies, particularly the Queensland Police Service, were operating informally, creating ambiguity about management responsibilities, such as ensuring that the use and disclosure of the footage was in accordance with the privacy principles. Each gap represents a risk, which if left unmanaged, could result in a privacy breach that could significantly affect members of the community. This review found this situation had arisen through a lack of corporate level direction and review and a lack of documented policies and procedures that addressed the complete spectrum of relevant considerations.

This report recommends agencies across the board review their camera surveillance systems, to ensure privacy issues have been considered and that the systems are managed actively in accordance with sound and well documented policies and procedures. Specific recommendations have been made to assist government agencies to ensure that government camera surveillance systems recognise and protect individual privacy through compliance with the requirements of the *Information Privacy Act 2009* (Qld) (IP Act).

## 2 Recommendations

---

*It is recommended that:-*

### **Recommendation One**

Every government agency implements a system for tracking the number and details of surveillance cameras operated by the agency.

### **Recommendation Two**

Before an agency implements or expands camera surveillance systems, the agency obtains and evaluates evidence regarding the effectiveness of camera surveillance for the purpose identified, the ongoing costs and benefits of camera surveillance systems and the features of camera surveillance systems required for the system to fulfil the agency's purposes.

### **Recommendation Three**

Agencies ensure the management of their camera surveillance systems is consistent with their given reasons for the camera surveillance, both in documented policies and procedures, and in practice.

### **Recommendation Four**

Agencies ensure that information collected by the camera surveillance system is complete and up-to-date, including through clear policies and procedures for storage, retention and disposal of camera surveillance footage, and training.

### **Recommendation Five**

Agencies review the extent to which they have provided notices to the community about the use of camera surveillance, particularly in the immediate vicinity of the cameras.

### **Recommendation Six**

Agencies ensure data security practices protect camera surveillance footage against loss, unauthorised access, disclosure, modification or other misuse and that these practices are described in documented policies and procedures.

### **Recommendation Seven**

Agencies publish information about their holdings of camera surveillance footage including the currency of the footage, so that individuals can discover if there is any camera surveillance footage held by the agency which might contain images of them.

### **Recommendation Eight**

Agencies provide publicly accessible information, preferably in the vicinity of each of the cameras they operate, informing the community of the camera's ownership and a point of contact for the relevant agency.

### **Recommendation Nine**

Agencies ensure they have policies and procedures in place which detail how individuals can obtain from an agency any camera surveillance footage which contains images of them, subject to exemptions prescribed in the *Information Privacy Act 2009* (Qld).

### **Recommendation Ten**

Agencies actively inform the community of the presence of camera surveillance systems, the rationale for their deployment, the privacy safeguards for the system and the mechanism by which the community can apply for access to the surveillance footage.

### **Recommendation Eleven**

Agencies review the way in which camera surveillance footage is scanned and material extracted in response to requests for copies of the footage, and ensure this process is demonstrably consistent with the privacy principles.

### **Recommendation Twelve**

Agencies ensure policies and procedures are in place for use and disclosure of personal information that ensure that personal information is used for secondary purposes or disclosed only as provided for in the *Information Privacy Act 2009* (Qld), for example, with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes.

### **Recommendation Thirteen**

Agencies develop administrative arrangements for disclosure of information where this is usual practice, for example, a Memorandum of Understanding with the Queensland Police Service, and adopt a standardised request form which ensures disclosure of camera surveillance footage is in accordance with the privacy principles.

### **Recommendation Fourteen**

Agencies review contracts with private security contractors to ensure contracts bind the contractors to compliance with the privacy principles.

### **Recommendation Fifteen**

Agencies develop policies and procedures to ensure that any camera surveillance footage transferred overseas, for example placed on the internet, is done within a clear legislative authority.

## 3 Introduction

---

### 3.1 Background

The past decade has seen an increasing use of surveillance cameras, including Closed-Circuit Television (CCTV).<sup>1</sup> Queensland's *Information Privacy Act 2009* (Qld) (**IP Act**) came into force on 1 July 2009 (1 July 2010 for local government). The IP Act sets out privacy principles which deal with government agencies' collection, storage use and disclosure of personal information – which can include surveillance footage. The Office of the Information Commissioner (**OIC**) has conducted an audit of camera surveillance usage by government agencies in 2011-12 to examine the extent to which the increasing volume<sup>2</sup> of surveillance footage is gathered and used in accordance with recent legislative requirements.

Government use of camera surveillance to promote safety and security is increasing world-wide. It has been estimated that there are 1.85 million cameras in the United Kingdom, which translates as being one camera for every 32 citizens.<sup>3</sup> Australia is following suit. In 2010, the Victorian Law Reform Commission reported:

*Public place surveillance is so extensive that it now affects the lives of nearly all Victorians. It is highly likely that our image will be captured by camera, and recorded, whenever we are walking down city streets, travelling on public transport, driving on freeways, visiting shopping centres or attending a major sporting event. People should know about these activities and appreciate that it is becoming increasingly difficult to remain anonymous in public places. The notion of blending in with the crowd is fast disappearing.*<sup>4</sup>

Similar comments have been made in a report of the Western Australian Auditor General.<sup>5</sup>

If Australia follows the same patterns of growth in the use of camera surveillance as has been observed in the United Kingdom,<sup>6</sup> in conjunction with increased awareness and

---

<sup>1</sup> Acronyms used in this report are listed in Appendix 1.

<sup>2</sup> Logan City Council's system camera surveillance data store in 2011 was 102 Terabytes (approximately half the data store of the world's largest library, the US Library of Congress). This storage is filled every 21-28 days. Logan Safety Camera Program Review 2001-2011, Logan City Council, page 11.

<sup>3</sup> Viewed at <http://www.securitynewsdesk.com/2011/03/01/how-many-cctv-cameras-in-the-uk/> on 12 March 2012.

<sup>4</sup> Victorian Law Reform Commission, *Surveillance in Public Places*, Final Report 18, May 2010, viewable at [http://www.lawreform.vic.gov.au/sites/default/files/Surveillance\\_final\\_report.pdf](http://www.lawreform.vic.gov.au/sites/default/files/Surveillance_final_report.pdf)

<sup>5</sup> Western Australian Auditor General's Report, *Use of CCTV Equipment and Information*, Report 9 – October 2011, viewable at [http://www.audit.wa.gov.au/reports/pdfreports/report2011\\_09.pdf](http://www.audit.wa.gov.au/reports/pdfreports/report2011_09.pdf)

concerns about personal information privacy, organisations using camera surveillance will need to satisfy higher community expectations regarding protections in place to manage privacy risks.

The IP Act provides a roadmap for government agencies in conducting its business while ensuring appropriate safeguards are in place to protect Queenslanders' personal information, to manage such risks and thus meet community expectations.

OIC has conducted the review and prepared this report to Parliament on its findings.

### **3.2 Reporting Framework**

The review has been conducted under section 135 of the IP Act, which includes conducting reviews into personal information handling practices of relevant entities, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally. It also includes assessing relevant entities' compliance with the privacy principles, which are provided in full in Appendix 2.

Under section 135 of the IP Act, the Information Commissioner is to give a report to the Speaker on the findings of any review, as appropriate.

### **3.3 Scope and objectives**

The objective of the review has been to examine and report on Queensland government agencies' use of camera surveillance (for example CCTV cameras) to:

- a. establish whether agencies comply with the prescribed requirements of the *Information Privacy Act 2009* (Qld) (IP Act)
- b. identify areas of good practice
- c. make recommendations to improve compliance with the IP Act.

The Terms of Reference for the review are provided in Appendix 3.

---

<sup>6</sup> Webster, W., 2009, *CCTV policy in the UK: reconsidering the evidence base*, Surveillance and Society 6 (1):10-22. viewable at <http://www.surveillance-and-society.org>

The review examined Queensland government agencies' use of camera surveillance with respect to information handling practices and compliance with the privacy principles<sup>7</sup> under the IP Act. This included an examination of:

- agency governance
- accountability and performance monitoring systems
- compliance with legislative requirements of the IP Act
- the extent to which the community is informed on the purpose for and the uses of each camera used for surveillance; and
- the extent to which the agency engages with the community about the implementation and use of camera surveillance and the handling of information gathered through camera surveillance.

This review did not examine covert surveillance<sup>8</sup> and nor did it examine mobile or temporary surveillance cameras.

### **3.4 Assessment process**

Evidence was gathered through the following processes:

- a. a survey of agency camera surveillance implementation and use
- b. in-depth compliance review of five agencies selected to provide a representative sample of agencies:
  - The Department of Communities<sup>9</sup>
  - Ipswich City Council
  - James Cook University
  - Logan City Council
  - Townsville City Council
- c. discussions with relevant staff and management

---

<sup>7</sup> The 'privacy principles' include sub-groups - the Information Privacy Principles, the National Privacy Principles, and obligations under section 33 and Chapter 2 Part 4 of the IP Act.

<sup>8</sup> The privacy principles do not apply to documents arising out of, or connected to covert activities – see Part 1 of Schedule 1 of the IP Act.

<sup>9</sup> The review covered the Department of Communities as it existed prior to the *Administrative Arrangements Order (No. 3) of 2012*, made by the Governor in Council on 3 April 2012, and published in the Extraordinary Government Gazette on 3 April 2012.

- d. observation of personal information handling practices
- e. examination of agency website and intranet; and
- f. review of statistical records/reporting.

The review was based on an assessment of the performance of the agency against the requirements in the IP Act.

Where the legislation stated that the agency must meet a particular requirement, that requirement was considered to be an auditable element of the legislation. The review tested whether or not agencies had complied with that requirement.

Where the legislation indicated that the agency should adopt a particular approach, the review made a qualitative assessment of the extent to which the agency had adopted that approach.

The survey was conducted by the Office of Economic and Statistical Research (OESR), who prepared a report on the survey findings. A copy of this report is provided in Appendix 4.

The remainder of the review was conducted by OIC. Comments were obtained from agencies reviewed in-depth on the draft report, as summarised in Appendix 5, and these responses were taken into account in the final report.

### **3.5 Reasons for using camera surveillance**

There are five cited<sup>10</sup> purposes for using camera surveillance systems.

- *prevent crime and disorder by acting as an effective psychological deterrent to potential offenders*
- *aid the detection of crime and disorder and enable a greater proportion of crime to come to the attention of police or security personnel*
- *enhance the apprehension and successful prosecution of offenders by enabling the effective deployment of officers and the gathering of evidence*
- *reassure the public and thus increase feelings of safety or reduce fear of crime;*  
*or*

---

<sup>10</sup> Allard, Wortley and Stewart, 2006; Barnard, 1988; Chatterton and Frenz, 1994; Dolahenty, 1999; Horne, 1996; Kruegle, 1997; Kyle and Aldridge, 1992; Phillips, 1999.

- *act as a general site management tool that assists police or security personnel to effectively manage locations.*<sup>11</sup>

The research has not found that camera surveillance necessarily delivers on these purposes. In particular, the effectiveness of camera surveillance as a deterrent to crime is in doubt.<sup>12</sup> One United Kingdom review concluded, after reviewing a series of studies into the impact of camera surveillance on crime rates, that it is a 'myth to assume CCTV reduces crime.'<sup>13</sup>

There is guarded support in the research literature<sup>14</sup> for the use of camera surveillance after a crime has occurred, for instance, in the investigation of crime or disorder; and in prosecuting offenders.<sup>15</sup>

Generally though, there is agreement by the researchers that camera surveillance is not a single answer for dealing with public safety and property protection. Rather, it can be useful when part of a suite of strategies, particularly if physical patrolling is also one of the strategies.<sup>16</sup>

<sup>11</sup> Wells, H. and Allard, T., *Crime and CCTV in Australia: Understanding the Relationship*, Faculty of Humanities and Social Sciences, Humanities & Social Sciences papers, Bond University Year 2006, viewable at [http://www.griffith.edu.au/\\_data/assets/pdf\\_file/0005/13379/crime-cctv.pdf](http://www.griffith.edu.au/_data/assets/pdf_file/0005/13379/crime-cctv.pdf)

<sup>12</sup> For example, a comprehensive report was prepared for the United States Congress on "*Preventing Crime: What works, what doesn't, what's promising*", which evaluated over 500 separate studies of crime prevention and drew conclusions about the crime prevention strategies where there was sufficient evidence to demonstrate that the strategy worked, and where the evidence was inconclusive. Although the report is old (1996) it is unique in its breadth and rigour. At the time of the report, the evidence for the effect of CCTV in preventing crime was inconclusive at best, and several studies showed that initial drops in crime when CCTV was introduced were not sustained over time.

<sup>13</sup> Webster, W., 2009, *CCTV policy in the UK: reconsidering the evidence base*, *Surveillance and Society* 6 (1):10-22. <http://www.surveillance-and-society.org> at page 17.

<sup>14</sup> For example, the Victorian Law Reform Commission summarised research in Australia and overseas about the uses of CCTV in crime detection and prevention, and found that one of its primary benefits was in investigating criminal behaviour (p61) but that there are concerns about how well CCTV works in preventing crime (pp 69-71). *Surveillance in Public Places*, Final Report 18, Victorian Law Reform Commission, 2010.

<sup>15</sup> The Western Australian Auditor General's report provided evidence in support of this usage, in a quote from the Chief Magistrate of Western Australia:

*CCTV is having an effect on the outcome of trials. It is a real asset for the Court in any kind of disputed fact. It is a central point from which, as a fact finder, you can say "I have seen that, there is no dispute that that happened". It has certainly increased the number of pleas of guilty.*

Western Australian Auditor General's Report, *Use of CCTV Equipment and Information*, Report 9 – October 2011, viewable at [http://www.audit.wa.gov.au/reports/pdfreports/report2011\\_09.pdf](http://www.audit.wa.gov.au/reports/pdfreports/report2011_09.pdf) at page 9.

<sup>16</sup> For example, the Western Australian Auditor General's report of the use of camera surveillance found that the proportion of offences per million passenger boardings had decreased from about 50 to under 40 incidents per million in the period 2002/03 to 2010/11, following the introduction of the Urban Security Initiatives Project in mid 2000. This project integrated camera surveillance into a coordinated security strategy, which included upgraded lighting and an increased number of officers with a rapid response capability as part of eight distinct security strategies. Western Australian Auditor General's Report, *Use of CCTV Equipment and Information*, Report 9 – October 2011, viewable at [http://www.audit.wa.gov.au/reports/pdfreports/report2011\\_09.pdf](http://www.audit.wa.gov.au/reports/pdfreports/report2011_09.pdf) at page 20.

Further research into expansion of camera surveillance in Australia has identified an additional motivation for camera surveillance.

*'Law and order' rhetoric has reverberated through the past decade of Australian politics (Hogg and Brown, 1998).<sup>17</sup> This has been no less true for local government politicians than their State and Federal counterparts. To promise ratepayers a CCTV system is to demonstrate that Council is 'tough on crime'.<sup>18</sup>*

Research has found that the mere presence of a camera surveillance system provides a measure of reassurance to the public and generates a perception of public safety.

For example, in a 2006 survey of 896 residents, business traders and commuters in the Gold Coast area in Queensland, an overwhelming majority of respondents supported the use of surveillance cameras to prevent both crime (a range of 93% to 97% of respondents) and terrorism in Australia (a range of 89% to 95% of respondents). Residents were 'very happy' (a range of 57% to 72% of residents) about having public space cameras on the Gold Coast. Business respondents agreed that more cameras should be installed in their respective central business districts (a range of 65% to 77% of business respondents).<sup>19</sup>

The perceived utility of camera surveillance by licensed premises is now reflected in the adoption of camera surveillance as part of the licensing framework under the *Liquor Act 1992*.<sup>20</sup> OIC is unaware of any evaluation of this strategy.

OIC acknowledges that camera surveillance may boost public confidence, and can have benefits for general site management, particularly as part of a suite of strategies which include a physical security presence. OIC further acknowledges the usefulness of camera surveillance footage in the detection and prosecution of offenders.

## The privacy principles

Any system which involves the collection and use of personal information by a government agency is subject to the requirements of the IP Act.

---

<sup>17</sup> Russell Hogg and David Brown, *Rethinking Law and Order*, Sydney: Pluto Press Australia Ltd, 1998

<sup>18</sup> Sutton, A. and Wilson, D., *Open-Street CCTV in Australia: The Politics of Resistance and Expansion*, Surveillance & Society, 2001, 2 (2/3), pages 310 to 322, at page 316 viewed at [http://www.surveillance-and-society.org/articles2\(2\)/australia.pdf](http://www.surveillance-and-society.org/articles2(2)/australia.pdf) on 19 March 2012.

<sup>19</sup> Wells, H. and Allard, T., *Crime and CCTV in Australia: Understanding the Relationship*, Faculty of Humanities and Social Sciences, Humanities & Social Sciences papers, Bond University Year 2006, viewable at [http://www.griffith.edu.au/data/assets/pdf\\_file/0005/13379/crime-cctv.pdf](http://www.griffith.edu.au/data/assets/pdf_file/0005/13379/crime-cctv.pdf) at page 46.

<sup>20</sup> For example, sections 51, 105 and 142AH of the *Liquor Act 1992*, Regulation 38A and associated prescribed forms and guidelines, such as Guideline 42.

These requirements do not prevent agencies from undertaking their legitimate business activities. The IP Act is not intended to prevent government agencies using camera surveillance for the purposes of ensuring public safety and security, or to prevent government agencies from informing the public about their camera surveillance operations.

What the IP Act does require is that government agencies implement safeguards for the handling of personal information, in pursuit of the broader aim that in the course of government business, agencies show respect for individuals' freedom to go about their lives without undue interference.<sup>21 22</sup>

In this respect, the requirements of the IP Act resemble any other framework that regulates government business activities: ensuring that government business operates according to a high standard against which Queenslanders can hold government accountable.

These requirements are set down in the privacy principles, which include the specific requirements listed in the 11 Information Privacy Principles (**IPPs**),<sup>23</sup> the obligations for when personal information is transferred overseas (section 33 of the IP Act) and when government agency services are conducted by non-government entities (Chapter 2, Part 4 of the IP Act). Section 27 of the IP Act requires government agencies to comply with the IPPs.

Cameras operated by Queensland Health and its bound contracted service providers are obligated to comply with the National Privacy Principles (**NPPs**) instead of the IPPs. This review consistently refers to the IPPs, in part because the five agencies showcased in the in-depth audit are subject to the IPPs.

However, the privacy obligations regarding camera surveillance for the IPPs are similar to the NPPs and the discussion concerning compliance will accordingly equally apply to Queensland Health as it does to all other government agencies. The equivalent NPP is provided in the heading of the discussion for each IPP.

### **3.6 Is camera surveillance footage 'personal information'?**

The IPPs are primarily concerned with the handling of personal information in documents.

---

<sup>21</sup> See Article 17 of the International Covenant on Civil and Political Rights viewable at <http://www2.ohchr.org/english/law/ccpr.htm>

<sup>22</sup> Australian Law Reform Commission Report no. 108, viewable at <http://corriganaustlii.edu.au/au/other/alrc/publications/reports/108/1.html#Heading152>

<sup>23</sup> Provided in full in Appendix 2.

‘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 reasonably be ascertained, from the information or opinion.*

A photograph, live or still, of an individual does not in itself usually identify the person. Rather, in order to identify a person in a photograph, the visual image must be associated with other information or knowledge. That source of other information or knowledge is context-specific. A person viewing footage of a crowd of people would only be able to identify persons known to them from personal experience, or who had come to their attention through previous publicity.<sup>24</sup> If the footage is of sufficient quality, a person with the necessary knowledge would be able to reasonably ascertain the identity of an individual from camera surveillance footage. Quality will be determined by factors such as:

- the size of the image of an individual
- the level of detail of the image
- the position of the person to the camera; and
- the degree to which the individual’s face or other identifying characteristics are visible.

If a person captured in footage was identifiable, the footage would reveal information ‘about’ that individual, not least that they were present in that space at that time and any actions performed by the individual in that space. Accordingly, camera surveillance footage has the potential to constitute personal information in a document and the obligations in the privacy principles apply.

The meaning of a ‘document’ is defined in the *Acts Interpretation Act 1954*, and includes:

*Any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device).<sup>25</sup>*

Camera surveillance footage constitutes a ‘document’ for the purposes of the IP Act.

---

<sup>24</sup> For example, if the footage recorded the visit of a well-known sportsperson and Australian personality to a suburban shopping precinct, a significant number of people would be able to identify the sportsperson from the footage.

<sup>25</sup> Section 36.

## 4 Privacy – A systemic issue

---

### **Background**

#### **Prevalence of camera surveillance**

In order to establish the degree to which people's privacy can be impacted by the use of camera surveillance, a component of this review was to establish the extent to which camera surveillance was being used by government agencies. A survey of government agencies was conducted that explored levels of usage, the purpose of usage, and accompanying compliance with the IPPs.

#### **General Management and Documentation of Policy**

The requirements of the information privacy principles can be satisfied largely through the development of clear, written policies and procedures that embed privacy considerations into the fabric of the day-to-day operations of an organisation. This also leads to consistent quality decision-making.

*Many of my recommendations involve the development and implementation of policies. By policies, I mean any written practices and procedures of a regulator, regardless of their title (for example, 'operational guidelines' are policies). Policies are a guide to consistency in the exercise of discretion, one of the key elements of good decision-making.*

Tips and Traps for Regulators, November 2007, Queensland Ombudsman.

### **Key findings**

- Over 20,000 cameras have been purchased and are being operated by Queensland government agencies.
- Over one quarter (26.3%) of agencies reported in the survey that they had no policies or procedures governing their surveillance camera systems. Over one half of agencies (53.9%) had five or more documented policies or procedures.

## 4.1 Prevalence of Camera Surveillance

A necessary part of this review was to establish the extent to which camera surveillance was being used by government agencies. A survey of government agencies was conducted, which explored levels of usage, the purpose of usage, and compliance with the IPPs. The survey was administered by the Office of Economic and Statistical Research (**OESR**) on behalf of OIC between November 2011 and January 2012.

The survey was sent to 176 agencies<sup>26</sup> identified in OIC's previous electronic audit as being agencies to which the IP Act applies, encompassing departments, local governments, statutory authorities and universities. 122 completed questionnaires were received, a response rate of 69.3%.<sup>27</sup> OESR advised that this response rate was high for a web survey, and indicated this high response rate would have minimised non-response bias and produced representative results.

OESR produced a full report on the survey results, provided at Appendix 4. Almost two thirds of responding agencies operated surveillance cameras (76 out of 122 agencies, 62.3%). Between them, these agencies operated over 20,000 surveillance cameras. Table 1 provides a breakdown of the number of cameras by agency type.

**Table 1**  
**Number of surveillance cameras operated by agency type.**

Type of agency	Number of cameras	Percentage	Agencies responding
Department	13,631	67.1	9
Local Government	3,609	17.8	35
Public Authority	3,070	15.1	32
<b>Total</b>	<b>20,310</b>	<b>100.0</b>	<b>76</b>

This figure is understated, possibly to a significant degree, due to the limited responses of two departments. One department did not respond at all to the survey.<sup>28</sup> Another department responded, but its internal processing method for responding to the survey led to

<sup>26</sup> The original frame contained 179 agencies. Three were defined as out of scope, on advice that their responses would be encompassed within the response from a larger, parent agency.

<sup>27</sup> Significantly, one of the agencies subject to the in-depth review, James Cook University, did not provide a survey response.

<sup>28</sup> The Department of Employment, Economic Development and Innovation (**DEEDI**) did not respond. The survey was sent to an officer on long service leave whose emails were not being monitored. Upon the next DEEDI officer receiving the survey a five day time frame remained. Five days was insufficient time for an agency wide survey to be conducted and completed for such a diverse and regionalised agency. Accordingly, DEEDI regrettably advised it would not be providing a response to the survey, however had obtained a copy of the survey to use as a guide in any possible future camera surveillance audits.

a report to the survey that the agency operated only 20 cameras. The department subsequently provided information that one division of the department operated 348 cameras. However, it could reasonably be projected that the agency would operate many more cameras.<sup>29</sup>

During the administration of the survey, it was common for agency representatives to comment that the survey brought to light for the first time the extent of the use of camera surveillance within their agencies. This is understandable in large agencies. Cameras and monitoring equipment can be inexpensive, and this review found that they were often purchased in local sections or divisions within an agency, within a local expenses budget and expenditure delegation, without any need to advise central administration.

Having said that, this review found that a series of small purchases of camera surveillance equipment and systems had aggregated into significant property assets of agencies, which now need to be managed from a corporate perspective to ensure both compliance with relevant legislation and minimisation of attendant risks. For future agency governance of camera surveillance systems, agencies need to implement a centralised system for capturing the number of cameras and relevant details about the camera surveillance systems.

### **Recommendation One**

It is recommended that:

Every government agency implements a system for tracking the number and details of surveillance cameras operated by the agency.

OESR categorised agencies' camera holdings according to small, medium and large camera installations, and found a relatively even number of agencies in each category. That is, a third of agencies had 1 - 10 cameras, a third had 11 – 100 cameras and a third of agencies operated over 100 cameras. Generally speaking, government departments operated more than 100 cameras (88.9% of departments) while local government councils (77.1%) and public authorities (71.9%) tended to operate 100 cameras or less.

<sup>29</sup> The Department of Education and Training (DET) reported the operation of 20 cameras in the category of public transport conveyances to the survey. Subsequently, DET advised OIC that 12 TAFEs operated 348 cameras. This did not include cameras that might be installed in schools, or other DET buildings. In response to the draft report, the department estimated that there would be approximately 152 schools which had surveillance cameras. Advice from the DETE School Security Advisors is that an accurate estimate of an average installation is between 8 and 12 cameras. This would lead to an estimate of there being between 1200 and 1800 cameras in schools.

There were noticeable differences between agencies that had large camera installations and agencies that had only a few cameras.

Agencies that operated more than 100 cameras appeared to be more likely to:

- capture footage of private property (44.0%), followed by agencies that operated a medium sized installation (33.3%) and a small sized installation (20.8%)
- have five or more documented policies/procedures in place (80.0%), compared to agencies with a small sized installation (41.7%) or medium sized installation (40.7%)
- provide training to staff (56.0%), compared to agencies that operated a small sized installation (25.0%) or medium sized installation (14.8%)
- cite more information and evidence to support the introduction of their camera surveillance systems than other agencies
- inform the community about their camera surveillance (80.0%), compared to agencies with a small sized installation (45.8%) and medium sized installation (44.4%)
- implement formal management procedures for security of camera footage
- have an administrative arrangement with the Queensland Police Service (72.0%), compared to agencies with medium sized installation (44.4%) or a small sized installation (8.3%); and
- have a private sector contractor operate their camera surveillance systems (56.0%), compared to agencies that operated medium sized installation (18.5%) or a small sized installation (8.3%).

The exception was that agencies that operated a medium sized installation of 11 – 100 cameras (86.7%) were most likely to have a formal written agreement or established procedure to provide other agencies with access to footage, compared to agencies with over 100 cameras (80.0%) or agencies with a small sized installation of 1 – 10 cameras (60.0%).

This means that issues identified throughout this report are more likely to need attention from agencies with medium to small installations of cameras, and these are more likely to be local councils or statutory authorities.

## **4.2 General Management and Documentation of Policy**

Of the 76 agencies which reported operating surveillance cameras, there was a polarity of responses around the degree of formalised policy documentation governing the systems. Over one quarter (26.3%) had no policies or procedures governing their surveillance camera systems. On the other hand, over one half of agencies (53.9%) had five or more documented policies or procedures.

Policies commonly developed were about instructing staff on the operation of the cameras (56.6% of agencies), retention and disposal of footage (51.3% of agencies), accessing footage (57.9% of agencies) and disclosure of footage to others (59.2% of agencies). Although there were documented procedures for the operation of the cameras, less than a third of agencies provided training to their staff on the operation of the cameras.

Government departments were more likely to have five or more policies in place (88.9% of departments) compared to local governments (51.4% of local governments) or public authorities (49.9% of public authorities). Agencies with large installations of cameras were more likely to have policies and procedures in place.

As discussed throughout this report, a common finding was that practices on the ground were generally sound due to the operational decisions of the front line staff. However, these practices had not been reviewed from a corporate perspective, and so occasionally the front line staff developed a practice which was inappropriate or outside the requirements of the legislation (for example, a practice of deleting material that should have been retained, failing to adequately communicate the presence of camera surveillance or a practice of refusing to allow individuals to access camera surveillance footage of the individual's personal information when it should not have been refused).

This lack of corporate review was reflected in the general lack of formal documented policies and procedures. Apart from allowing local practices to drift or develop outside of proper practice, the lack of documentation also allowed for inconsistent decision making, inadequate handover to new officers and agencies unable to inform themselves about the effectiveness or otherwise of their management of the camera surveillance system. Agencies were accordingly vulnerable to 'brain drain' – valuable operational knowledge being lost when relevant staff left the agency. Many of the specific findings of this review pointed to the general need for a review of the systems from a privacy perspective, to

culminate in the production of documented policies and procedures to ensure the systems are managed effectively with privacy in mind, through compliance with the IP Act.

Sections 5-12 of this report include recommendations that agencies documents policies for the management of camera surveillance systems to address specific requirements of the IP Act.

## 5 Information Privacy Principles 1 - 3 – Collection

---

### Privacy requirements

**IPP1 Collection of personal information (lawful and fair).** Agencies need to have a clear, lawful purpose for collecting personal information via camera surveillance.

**IPP2 Collection of personal information (requested from individual).** Agencies need to take reasonable steps to ensure an individual is generally aware of the reasons and authority for collecting personal information, and any usual practices for disclosing the information to another entity.

**IPP3 Collection of personal information (relevance).** An agency must ensure that personal information collected by surveillance cameras is relevant for the purpose for which it is collected.

### **Information Privacy Principle 1 (IPP1) (equates to National Privacy Principle 1)**

IPP1 requires that when agencies collect personal information through camera surveillance:

- the footage is collected for a lawful purpose directly related to a function or activity of the agency
- the collected footage is necessary for the fulfilment of that purpose; and
- the collection is not unfair or unlawful.

In practice, agencies have a range of functions from those that are unique and finely focussed<sup>30</sup> to others which are defined in the broadest terms. Many of the functions are defined in legislation.

Additionally, some functions will be common to all government agencies; these functions include the obligations to:

- provide a safe workplace
- deal with government assets responsibly (including the reasonable safeguarding of those assets); and

---

<sup>30</sup> For example, only the Department of Transport and Main Roads can issue Queensland Driver Licences.

## **Privacy requirements**

- ensure the safety of the public when obtaining the services of the agency.

An agency should be able to clearly articulate and communicate the direct relationship between the use of camera surveillance and the agency's lawful functions.

If an agency does not use the footage itself but instead collects it on behalf of another agency or if the agency is 'data-mining' the footage – collecting information for no immediate defined purpose - the agency is potentially breaching the obligations in IPP1.

To avoid a claim that the surveillance is occurring unfairly, it is common practice to inform persons that surveillance cameras operate within the immediate vicinity. This is in addition to the requirements of Information Privacy Principle 2 (IPP2) (which equates to National Privacy Principle 1) - see following.

### **Information Privacy Principle 2 (IPP1) (equates to National Privacy Principle 1)**

IPP2 requires that when an agency collects personal information from the individual themselves, the agency takes reasonable steps to make the individual generally aware of:

- the purpose for the collection
- any lawful authority for the collection
- to whom the agency may pass the information onto; and
- as appropriate, to whom the information may be passed in turn onto.

The above information can be contained in a succinct paragraph termed a 'collection notice'. The 'collection notice' for camera surveillance would be expected to consist of a sign posted in the vicinity of the camera which informs the community of the purpose for the surveillance.

The following notice of the Western Downs Regional Council is an example of a camera surveillance collection notice:

*'Western Downs Regional Council is collecting your personal information on a closed circuit television system (CCTV) in this area. The personal information collected is being used for the purposes of public safety, crime prevention and detection. Your personal information will only be accessed by persons who have been authorised to do so. This information may be provided to the Queensland Police Service for law enforcement purposes. Your information will not be given to*

## **Privacy requirements**

*any other person or agency unless required by law. Your personal information is handled in accordance with the Information Privacy Act 2009. Enquiries in relation to this notice may be directed to Western Downs Regional Council by calling ....*

Regardless of the IPP2 obligations, it is self evident that the deterrent effect of camera surveillance arises from persons being aware that their behaviour is recorded and that they modify that behaviour accordingly. The advertisement and/or dissemination of information about camera surveillance assists that awareness.

Additionally, the recorded images can be the personal information of individuals and they have a right to apply to access the footage. This right can only be exercised if the individual knows which agency is responsible for a particular camera - which is not always immediately obvious - and they can contact that agency to request access. As demonstrated in the example above, this information can be easily incorporated into the collection notice.

### **Information Privacy Principle 3 (IPP3) (equates to National Privacy Principle 1)**

IPP3 requires that when an agency collects personal information, the agency must take all reasonable steps to ensure that the information is both relevant for the purpose for which it is collected and complete and up-to-date.

Once an agency has clarified its reasons for considering camera surveillance, then in order for the footage to be relevant, it must relate to the articulated reasons for the camera surveillance. An agency should be able to point to evidence supporting the use of camera surveillance for that purpose, and for the way in which the camera surveillance should be used. If for example, the purpose of a particular camera is to record evidence of vandalism to agency property (for example, graffiti), the cameras must capture both the property and any incidents of vandalism.

Judicious choices about the placement of cameras, the type of camera used and the quality of the image<sup>31</sup> will enable the delivery of the intended purpose.<sup>32</sup>

IPP3 also requires that the extent and methodology of collection must not be an

<sup>31</sup> For example, if the history of incidents shows damage is occurring largely at night and the camera system is not capable of sufficiently recording night footage, the captured information may not be relevant to the purpose for installing the camera.

<sup>32</sup> Agencies should be mindful of the potential for a privacy complaint to be made concerning their obligations to comply with the privacy principles. Robust communication with the community can forestall allegations of non-compliance.

## **Privacy requirements**

‘unreasonable intrusion’ in the private lives of people. For camera surveillance, this principle will be enlivened when footage is unnecessarily captured of private property. If for example, a camera routinely records activities within a private residence’s backyard and no articulated purpose is served by this surveillance, this could well be considered to be, an ‘unreasonable intrusion’ into the relevant person’s domestic affairs.<sup>33</sup>

For footage to be complete and up-to-date, systems for managing the footage must provide for proper policies and procedures for the footage’s storage, retention and disposal.<sup>34</sup>

## **Key findings**

- Agencies identified multiple reasons for installing surveillance cameras, with the most common being to protect property (89.5% of agencies). Agencies also cited crime prevention (77.6% of agencies), public safety (76.3% of agencies) and crime investigation and enforcement (64.5% of agencies).
- There is a lack of clarity within agencies about a primary purpose for operating their camera surveillance systems.
- Agencies have generally not focussed on communicating their ownership of cameras or the purposes, logistics and administrative procedures of camera surveillance systems to the community.
- Agencies reports in the survey identified that agencies did not consistently undertake research before deciding to introduce camera surveillance systems (only 40.8% of agencies had undertaken research).

---

<sup>33</sup> Agencies should also be aware of the potential application of section 227A of the *Crimes Act 1899*; this section states:  
**227A Observations or recordings in breach of privacy**

(1) A person who observes or visually records another person, in circumstances where a reasonable adult would expect to be afforded privacy—  
(a) without the other person’s consent; and  
(b) when the other person—  
(i) is in a private place; or  
(ii) is engaging in a private act and the observation or visual recording is made for the purpose of observing or visually recording a private act;  
commits a misdemeanor.

<sup>34</sup> For information on retention and disposal refer to Queensland State Archives *Guideline for Managing Closed Circuit Television (CCTV) Records* and accompanying public records briefs at <http://www.archives.qld.gov.au/Recordkeeping/Digital/Pages/AudioVisual.aspx>

### **Key findings**

- In many cases agencies have implemented camera surveillance without obtaining objective quantifiable data about community attitudes to camera surveillance; about the effectiveness of camera surveillance alone or as part of a larger strategy for crime prevention; or about the costs and benefits of operating camera surveillance.
- The siting of cameras and their operation did not always yield footage that was useful for the purpose installed.
- Agencies routinely captured footage of private property for no legitimate purpose, but there was evidence that they were mindful of the privacy implications of this practice.
- Around half of the agencies surveyed had policies and procedures for the storage, retention and disposal of the footage, and less than a third of agencies provided training to their staff in their policies and procedures.

## **5.1 Introduction**

In order to test agencies' ability to clearly articulate the direct relationship between the use of camera surveillance and the agency's lawful functions (adoption of IPP1), the agency survey asked '*What were the reasons for installing the camera surveillance system(s)?*' and '*Does your agency use the surveillance footage for any other reasons?*'.<sup>35</sup>

The survey also asked about notification provided to the people about the use of camera surveillance, by asking '*Does your agency actively inform the community about the surveillance?*', '*When notifying the community about the surveillance, how is the information provided?*' and a question providing options for the information provided in any notices.<sup>36</sup>

In order to test whether or not agencies took all reasonable steps to ensure that the information was both relevant for the purpose for which it is collected and complete and up-to-date, the agency survey asked '*What information or evidence supported the introduction of your camera surveillance system?*' and about policies, procedures and training provided to support the camera surveillance system.<sup>37</sup>

---

<sup>35</sup> Questions 3.1 and 3.2.

<sup>36</sup> Questions 4.1, 4.2 and 4.3.

<sup>37</sup> Questions 2.1 and 2.2 and 3.3.

The case studies provided information as to the consideration given by agencies to the purpose of the collection of personal information through camera surveillance. During the case studies, OIC noted whether or not an agency was collecting information on behalf of another agency or 'data-mining' the footage, (potentially breaching the obligations in IPP1), and the extent to which agencies informed people that surveillance cameras operated within the immediate vicinity. The case studies provided information as to the consideration given by agencies to the placement of cameras, and the extent to which the camera placement intruded upon private property. Case study agencies provided information about training provided to staff in the policies and procedures for managing cameras.

## **5.2 Findings**

Agencies were asked why they had installed surveillance cameras. The survey permitted agencies to nominate more than one reason for doing so. The most common reason for installing surveillance cameras was to protect property (89.5% of agencies). Agencies also cited crime prevention (77.6% of agencies), public safety (76.3% of agencies) and crime investigation and enforcement (64.5% of agencies). Staff safety was cited by 14.5% of agencies as a reason for installing cameras. Agencies' responses were similar across agency types.

The strength of responses in multiple categories led OIC to compare stated reasons for installing cameras against other survey responses. The aim of this analysis was to refine OIC's understanding of the purpose for installing the cameras by identifying whether or not responses aggregated to favour one type of purpose over another.

In response to the survey questions about the installation of cameras, over half of the cameras (55.4%) were installed for monitoring within government buildings, compared with monitoring building precincts (15.8% of cameras), traffic areas (18.9% of cameras), public transport conveyances (1.5% of cameras) or other locations (9.8% of cameras). This supported the finding that property protection was the predominant aim.<sup>38</sup>

Results for crime prevention as a stated reason for installation of cameras (77.6% of agencies) contrasted with survey responses as to whether or not notices were reported as being placed in proximity to the cameras to maximise the cameras' deterrent effect. A public notice close to the camera was used by 19 out of the 43 agencies providing public notices (44.2% of agencies providing notices, 25% of agencies reporting that they operate security

---

<sup>38</sup> Please note that for the purpose of this calculation and other calculations regarding camera location, the locations of Department of Communities' cameras were estimated using a formula, in order to avoid skewing the findings.

cameras). 67.4% of agencies reported providing a notice in the general vicinity of the camera, and the remainder notified the public of the camera surveillance on request, through a publicly accessible document or via media releases.

The case studies found that a common end user of camera surveillance footage was QPS for its use in crime investigation and enforcement. In particular, footage from Townsville City Council seemed to be accessed almost exclusively by QPS - for post-incident investigation. Of the five agencies reviewed in detail, only Ipswich City Council had implemented a system which actively monitored the footage for crime prevention activities purposes.<sup>39</sup> In both Townsville and Ipswich, QPS had access to a single access-only monitor. There was the capacity for QPS to contact the relevant council and request that their monitor show a specific camera but in practice, where there was live monitoring, it would be the agency's staff who would contact QPS concerning a crime in progress or (in the case of Ipswich) a potential crime.

It is a commonly-held perception that the camera surveillance systems in themselves have a commensurate effect on preventing crime.<sup>40</sup> The three Councils reviewed in-depth identified a publicly-held perception that safety in public spaces was a Council responsibility and that accordingly, there was a role for Council in crime prevention and detection. Councils said that safety was best served by a partnership between Council and QPS, where Council provided infrastructure and crime prevention through environmental design and QPS provided the required law enforcement activities.

OIC acknowledges that there is no standardised framework for evaluating the impact of camera surveillance systems. There were efforts by the three Councils to present statistical evidence for the importance of camera surveillance in preventing crime, but the presented evidence was patchy. OIC is encouraged that some of the agencies reviewed in depth had set out to evaluate the effectiveness of camera surveillance systems in this respect. However in one case OIC noted what appeared to be inconsistencies and incorrect assumptions in relevant evaluation documentation that may have affected outcomes of the analysis and possibly conclusions about the effectiveness of the camera surveillance system in preventing crime.

Another Council, the Ipswich City Council keeps monthly statistics concerning the use of camera surveillance in arrests and these statistics were used to support the effectiveness of

---

<sup>39</sup> While Logan City Council also had live monitoring, the staff would contact QPS once an incident was underway.

<sup>40</sup> See for example the Logan City Council 2010 – 2011 Annual Report at page 36.

camera surveillance in preventing crime under the Safe City Program. The monthly statistical reports as at October 2011 showed an average of 33 arrests were made as a known result of the Safe City Program, with a total of over 6300 arrests as a known result of the Safe City Program since the program's inception. The statistics also described a significant contribution by the Safe City Program in locating people sought by QPS, dealing with emergencies and providing assistance or notifying QPS about incidents. However, the use of camera surveillance to investigate and prosecute criminal incidents is not necessarily the same as preventing crime.<sup>41</sup> While it is of obvious benefit for a victim of a crime to receive a rapid police response as result of notification through camera surveillance, prevention requires the camera system to have a deterrent effect and/or it be used for active intervention before the crime occurs.

In the case of Ipswich City Council's Safe City Program a crime prevention effect was primarily achieved by active monitoring in real time of potential criminal incidents in partnership with QPS. At interview, the Safe City Program staff gave a number of anecdotal examples of serious criminal activity that were completely prevented or thwarted by the use of camera surveillance to notify QPS and trigger a response. A distinction between Ipswich City Council and most other systems reviewed in depth was that within the Safe City Program camera surveillance was set up to be part of an active and integrated crime prevention and public safety strategy, with a strong component of physical patrol and intervention as opposed to the systems being used for the purposes of reporting crime and used for providing evidence for criminal prosecutions.

This point was well understood by camera operators interviewed. A consistent theme arising from the case study interviews was that camera surveillance contributed effectively to public safety if three conditions were met:

- that camera surveillance was part of a larger integrated crime prevention strategy
- the crime prevention strategy was primarily reliant on personal presence and intervention by police or security officers, before an incident occurred;<sup>42</sup> and
- camera surveillance was more effective if the monitoring staff were specifically trained and experienced.<sup>43</sup>

---

<sup>41</sup> OIC acknowledges an argument that the arrest and prosecution of a serial offender may have an effect of preventing future offending by that person, but it also acknowledges that obtaining hard evidence of this potential benefit would be a difficult exercise.

<sup>42</sup> The effectiveness of physical presence was particularly noted where the offending was fuelled by alcohol.

While this potential exists for all camera surveillance systems, it was observed to a large part only in the Ipswich City Council.

Another commonly held perception was that camera surveillance was perceived by the community as safeguarding their safety in public, although agencies had not tested the actual extent to which the community held this perception.

A significant finding of this review was the extent to which public perceptions of safety and the contribution of camera surveillance to enhanced safety had influenced agency decisions to install camera surveillance systems. The survey found that 39.5% of agencies installed cameras to increase the public's perception of safety, and 26.3% installed cameras in response to perceived public demand or expectation. Agencies reported during the case study reviews that they were strongly influenced to maintain and expend camera surveillance by the community's 'belief' in camera surveillance, even though staff within the agencies expressed doubts at interview about whether or not the benefits of camera surveillance outweighed the costs, and about the effectiveness of the system at all in promoting public safety.

The insufficiency of evidence supporting the introduction of camera surveillance was also a survey finding, where very low numbers of agencies had researched the effectiveness of camera surveillance before introducing it (40.8% of agencies), conducted privacy impact assessments (10.5% of agencies), or were responding to specific identified needs (24% of agencies). Once the cameras were installed, just over a third of agencies (36.8% of agencies) conducted evaluations of the existing surveillance camera systems. On this issue, OIC is not commenting on the strength of the evidence itself, but rather, on the agency's preparedness to make a significant commitment to camera surveillance in the absence of evidence about its value or impact.

This review noted that interviewees from case study agencies tended to fall into one of two camps regarding the efficacy of camera surveillance in promoting public safety; either:

- holding a strong personal belief in camera surveillance systems as a means for promoting public safety, irrespective that they could not identify objective evidence for the effectiveness of the systems in preventing crime and promoting public safety; or

---

<sup>43</sup> For this reason, many agencies outsourced the monitoring function to specialist security organisations.

- despite their own personal beliefs, recognising the need to accommodate community and political calls for ongoing use and expansion of camera surveillance, irrespective of arguments and/or evidence of the value of camera surveillance.

The lack of evidence-based decision making had impacts not only in whether or not to install or expand camera surveillance systems, but also in how well or poorly the systems were run. For example, the case studies demonstrated that the placement of cameras did not always provide relevant footage. Particularly in the case of Townsville City Council, some cameras were located within the canopies of trees or on street corners where poles obstructed much of vision. Some cameras captured the canopies of buildings or focussed on buildings with little or no significance. Cameras set for automatic pan would often capture little more than footpaths or sky. Other cameras were broken or the lens was so obscured by dirt that no detail could be recorded. These cameras were replaced automatically, without first ensuring the camera location would lead to the capture of relevant footage.

This was reflected in the relatively low rate of usable footage supplied to QPS on request. Between 12 July 2011 and 21 February 2012, 96 requests were made to the Townsville City Council for footage – all from the QPS. 57% of these requests revealed ‘no usable footage’ for reasons such as:

- camera was focussed elsewhere – 44%
- no camera in the relevant area – 20%
- no footage recorded – 16%
- non-operational camera – 6%

A well monitored camera surveillance system, preferably where the pan and zoom functionality is controlled by an operator has the best chance of capturing relevant footage. The operators are also well placed to report on non-functional cameras. However, the agencies reviewed in-depth did not generally monitor the cameras or, as in the case of the Townsville City Council, had discontinued monitoring to save costs.

There were two other issues explored as part of checking the adoption of IPP1 and IPP3 – the capture of private property and whether or not the footage was complete and up-to-date.

### *Public vs. private*

Approximately one third of agencies operated cameras which captured footage of private property. This was most likely for local governments (45.7%) or for agencies with a large camera installation (44% of the agencies operating more than 100 cameras).

To their credit, the audited agencies that took part in the case studies were aware of this practice and took a variety of steps to minimise their capture of private property. These steps included:

- Logan City Council digitally masking some windows and doorways and making some owners aware that their property was being inadvertently surveyed.
- Ipswich City Council carefully siting cameras so that they did not capture the interior of some buildings.
- The Department of Communities installing physical privacy screens in some sensitive areas.

### *Ensuring the camera surveillance footage was complete and up-to-date*

In response to questions about the management of the footage, around half of the agencies reported that they had documented policies and procedures:

- to give staff instructions on operating the surveillance camera system (56.6% of agencies)
- to manage the surveillance camera records (44.7% of agencies); or
- for the retention and disposal of surveillance camera footage (51.3% of agencies).

31.6% of agencies reported providing training to staff in surveillance camera system policies and procedures.

It is noted that during the course of the in-depth reviews of five agencies, some agencies had specific and different views on whether the record-keeping requirements of the *Public Records Act 2002* applied to surveillance footage in their particular circumstances regarding collection and use. Such agencies therefore took different approaches to the retention and disposal of footage which, as discussed later in this report, has implications for compliance with aspects of specific IPPs.

OIC has advised Queensland State Archives (**QSA**) that some confusion was noted during the course of the review. QSA responded that its October 2010 *Guideline for Managing*

*Closed Circuit Television (CCTV) Records (Guideline)* provides advice assisting agencies meet their information management and recordkeeping obligations concerning camera surveillance systems<sup>44</sup>. QSA further stated that in order to clarify requirements for the retention and disposal of camera footage, QSA will consider re-issuing advice on this issue including the CCTV checklist from the Guideline to assist agencies..

### 5.3 Analysis and Conclusion

Agencies need to have a clear, lawful purpose for collecting personal information via camera surveillance.

The survey across all government agencies found that the most common reason for installing surveillance cameras was to protect property (89.5% of agencies). Agencies also cited crime prevention (77.6% of agencies), public safety (76.3% of agencies) and crime investigation and enforcement (64.5% of agencies). These purposes were clear and clearly within the ambit of government. A specific purpose also identified in the course of this review was the installation of camera surveillance in the youth detention centre to monitor the safety and wellbeing of young people and others and to provide the level of security required within a detention centre.

However, taken together with other survey responses and the evidence countering the proposition that crime **prevention** was a real end benefit of camera surveillance as a standalone strategy, three dominant purposes for government use of camera surveillance emerged from the review:

- protection of government property
- assisting QPS in detecting and prosecuting offenders after crimes had been committed; and
- boosting public confidence in government's efforts to provide for public safety and good order.

The fact that QPS was a primary 'end user' of the camera surveillance system and footage raised the question as to whether or not agencies were, in effect, collecting the footage for usage by another agency, rather than for a directly related function of their own.

However, in the case of local government for example, in some cases there are strategies and other documentation that outlines a formal or informal partnership with QPS to reduce

---

<sup>44</sup> Available at [www.archives.qld.gov.au](http://www.archives.qld.gov.au)

crime. This was for a number of objectives including public safety, but also to ensure continued and new investment in the local government area as a safe place to work and live. OIC considers that arguments can be made on a number of fronts for local governments having responsibility for the management of public spaces in addition to government agencies' general interests in the protection of government property. For these reasons, the implementation and use of camera surveillance systems would fall within the ambit of IPP1. Whilst satisfied that the collection of personal information by camera surveillance is lawful and fair in general, OIC remains concerned about the extent to which the legitimate purposes of camera surveillance might be overstated or stretched as a result of unsupported promotion of the preventive value of the systems.

Objective, quantifiable data about camera surveillance can enable agencies to link camera use to the agencies' legitimate purposes; for example:

- What are community attitudes about camera surveillance and to what extent does the community believe that camera surveillance promotes public safety?
- Would this perception be affected by the knowledge that, in the large part, the cameras record incidents of crime rather than being used as a tool to actively prevent crime?
- Does camera surveillance in itself prevent crime? Does it prevent crime only as part of a larger strategy? If only as part of a larger strategy, what are the essential elements of the larger strategy?
- As part of deterrence of crime and general management of public order, have agencies audited the extent to which they notify people of the use of camera surveillance?
- What are the real costs and benefits of camera surveillance, taking into account the costs of ongoing maintenance, the costs of monitoring footage and the costs of extracting footage to assist in investigation and prosecution?

Clarification of the purpose for camera surveillance, good evidence about the utility of camera surveillance in meeting that purpose and then careful consideration of how the system should be configured to meet that purpose are all elements of ensuring that camera surveillance footage is relevant.

As surveillance by CCTV can amount to a serious intrusion into the private lives of citizens, it is recommended that agencies evaluate whether or not the objectives behind introduction have been achieved and review the cost/benefit in using this technology in order to justify any ongoing privacy infringement.

The relevance of camera surveillance to the stated purpose was of concern. OIC considers that in order to work within the requirements of IPP3, agencies need to clarify their agenda and ensure that the installation, development and operation of the camera surveillance system is consistent with that agenda.

With respect to the issue of the capture of personal information by the camera surveillance beyond that required for the agency's functions, OIC did not find evidence that this was an issue of concern. IPP3 does not state that personal information of a domestic nature can never be collected; rather it requires that the collection not be an unreasonable intrusion. In some situations – for example where a single camera is viewing an entire traffic intersection, it may not be unreasonable that footage of some private property would be captured at the edges of the intersection. This review demonstrated that, from an operational standpoint, agencies were careful of the capture of private property and took steps to manage this issue.

### **Recommendation Two**

It is recommended that:

Before an agency implements or expands camera surveillance systems, the agency obtains and evaluates evidence regarding the effectiveness of camera surveillance for the purpose identified, the ongoing costs and benefits of camera surveillance systems and the features of camera surveillance systems required for the system to fulfil the agency's purposes.

### **Recommendation Three**

It is recommended that:

Agencies ensure the management of their camera surveillance systems is consistent with their given reasons for the camera surveillance, both in documented policies and procedures, and in practice.

Agencies also need to ensure that information collected by the camera surveillance system is complete and up-to-date. This is a major area for improvement. Around half of the agencies surveyed had not yet developed policies and procedures for storage, retention and disposal of camera surveillance footage, and two-thirds of the agencies surveyed had not yet provided training to staff in these policies and procedures. Agencies need to give careful consideration to retention and disposal practices to ensure they meet operational requirements whilst meeting requirements under the IP Act and the *Public Records Act 2002*.<sup>45</sup>

#### **Recommendation Four**

It is recommended that:

Agencies ensure that information collected by the camera surveillance system is complete and up-to-date, including through clear policies and procedures for storage, retention and disposal of camera surveillance footage, and training.

Just over half of the agencies reported actively advising the community of camera surveillance, and only a quarter of agencies reported placing a collection notice in the immediate vicinity of the cameras. Better notification to the community would ensure that the use of cameras was perceived as fair, and it would also seem to be a positive step in deterring or preventing crime or disorder. Providing information to enable individuals to apply for access to footage promotes openness and transparency about agencies' use of camera surveillance.

#### **Recommendation Five**

It is recommended that:

Agencies review the extent to which they have provided notices to the community about the use of camera surveillance, particularly in the immediate vicinity of the cameras.

<sup>45</sup> For information on retention and disposal refer to Queensland State Archives *Guideline for Managing Closed Circuit Television (CCTV) Records* and accompanying public records briefs at <http://www.archives.qld.gov.au/Recordkeeping/Digital/Pages/AudioVisual.aspx>

## 6 Information Privacy Principle 4 – Data storage and security

---

### Privacy requirements

**IPP4 Storage and security of personal information.** Surveillance camera footage must be stored so that it is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.

### **Information Privacy Principle 4 (IPP4) (equates to National Privacy Principle 4)**

Once an agency has recorded camera footage, IPP4 requires that the agency must ensure that the footage is protected against loss, unauthorised access, disclosure, modification or other misuse. This is an absolute obligation; there is no 'reasonableness defence'. If an agency for example, copies footage of an incident to a hardcopy disk but then loses the disk, this will be an automatic breach of IPP4.

If the footage is provided for legitimate purposes to another agency or person – for example if it is provided to the Queensland Police Service for their use in law enforcement - IPP4 also obligates the agency to take reasonable steps to prevent unauthorised use or disclosure of that footage by the other agency. While this obligation does have a reasonableness element, the agency should have a demonstrable indication that this obligation has been fulfilled; a mere reliance on the bona fides of the recipient agency may not be sufficient to fulfil this obligation.

If an agency is going to regularly provide footage to a second agency, an appropriately comprehensive Memorandum of Understanding between the two agencies can address this obligation. In the case of irregular or one-off provisions, a clear declaration of the terms under which the footage is provided can satisfy this obligation.

Security requirements will differ depending on the type and amount of personal information held by the agency. The whole-of-government Information Standard 18 provides guidance in this area. Security measures can include:

- **physical** - locks and swipe cards for monitoring rooms/areas and data storage areas, carefully placing monitors and/or using barriers and screens so that the live footage cannot be viewed by unauthorised persons

### **Privacy requirements**

- **electronic** - passwords for accessing the monitoring systems including access, retrieval and copy of the data, encryption of the data; and
- **operational** - restricting access to stored data on a needs basis and having a standardised auditable process for when access is provided.

If camera surveillance footage is a public record, then the requirements of the *Public Records Act 2002* intersect with IPP4 to create legislative obligations about the retention of the footage (and consequently the ability of individuals to access footage).<sup>46</sup> Deletion of any footage which is a public record in a way that is not permitted under the *Public Records Act 2002* would be incompatible with the requirements of IPP4 to protect the footage against unauthorised loss or modification.

### **Key findings**

- In the survey, most agencies (88.2% of agencies) reported that they stored the camera surveillance footage in their own facilities.
- Most agencies reported in the survey that they only allowed individuals to access the footage if they were authorised to do so (88.2% of agencies).
- Agencies have generally implemented data security practices, and while these practices are operationally sound, these practices are not always well documented.

## **6.1 Introduction**

In order to test whether or not surveillance camera footage was protected against loss, unauthorised access, use, modification, disclosure or any other misuse, the agency survey asked '*Where is your surveillance camera footage stored?*' and prompted agencies to nominate options they used to manage access to the footage.<sup>47</sup>

The case studies also provided information as to data storage and security measures adopted by agencies for their own use and on disclosing information to other agencies.

---

<sup>46</sup> Ibid.

<sup>47</sup> Questions 5.1 and 5.2.

## 6.2 Findings

Most agencies (88.2% of agencies) reported that they stored the camera surveillance footage in their own facilities, and only allowed individuals to access the footage if they were authorised to do so (88.2% of agencies). Protections included password protection (68.4% of agencies), physical security (64.5% of agencies) and data encryption (11.8% of agencies). Agencies with large installations of cameras or with five or more policies were also more likely to have implemented more formal management procedures for data security than agencies with smaller installations or fewer policies.

The survey identified nine agencies that did not confirm that individuals could only access footage if authorised to do so. This suggested a lack of appropriate control. A closer examination of responses from the individual agencies revealed that only two of those agencies reported no data security measures at all. The seven agencies with data security measures had adopted between one to four of the seven data security measures described in the survey. This could be interpreted to mean that these agencies were not oblivious to the importance of data security, but either had not adopted a full set of measures or had not adopted measures with enough rigour to enable them to report on the full range of data protection strategies. For example, people within an agency might generally have known who could access the footage, but the agency might not have been able to state that there was a formal authority provided to those people, or that access was strictly limited to these persons.

The agencies reviewed in-depth had taken care with data security, and had generally adopted security strategies such as password protecting access to data, limiting access to the computer records, ensuring monitors were located outside of the public view, limiting the staff members who could view the footage and ensuring that the computers on which the data was stored were in locked rooms. Agencies also demonstrated caution in accepting and responding to requests for data, including requests from QPS.

The obligation to prevent unauthorised access applies not only to the stored footage but also to the 'live' images. A member of the public who can view a camera monitor located in a non-public area is doing so without authorisation. This was an area which the five reviewed agencies performed well. The mechanisms varied between not siting monitors in public areas, to having designated secure areas where the monitors were located to arranging the

workspace so that visiting members of the public could not see the monitors or in one case, staff themselves erecting a curtain barrier between the monitors and public areas.

It emerged that an issue for all agencies was the operational need to reduce the amount of camera surveillance footage because of the potential demands on digital storage capacity. OIC found the agencies reviewed in-depth were deleting camera surveillance footage on the basis that digital storage capacity was reached.

Of particular concern was that some agencies were deleting digital footage that was extracted and made into a hard copy in response to a request, even though it was generally acknowledged that this type of digital footage was a public record. In part, this arguably reflects a system that has developed through operational practice and procedure rather than by agency leadership on governance.

### **Retention of camera surveillance footage**

As part of OIC's communication with QSA on this issue, QSA has advised that agencies should adopt a risk based approach when assessing how long to keep camera surveillance footage. This risk management approach is considered to be best practice (although not a legislative requirement). When making decisions on how long to keep camera surveillance footage, QSA stated that consideration should be given to local security issues and circumstances, together with priorities established by Government as well as those of the individual public authority.

QSA has identified that a relevant factor to determine how long camera surveillance footage should be kept is consideration of how long after an incident occurs that notification is typically received. Where, for example, incidents are known immediately in a control room, and the records immediately retrieved, QSA stated that consideration be given to the camera surveillance footage being kept for a shorter period of time.

Conversely, where incidents may not be reported or noticed for days/weeks, or it may take a significant time for the record to be retrieved from a recorder (for example, the recorder is mounted to a vehicle), QSA's recommendation is that the camera surveillance footage be retained for a longer period.

Where surveillance footage is accessed and/or copied (for example, when extracted camera surveillance footage is provided to the QPS for evidentiary purposes in a court proceeding),

QSA stated a view the footage is a public record and as such, must be deal with according to the General Retention and Disposal Schedule for Administrative Records<sup>48</sup> or alternatively, an agency / sector specific Retention and Disposal Schedule that has been approved by the State Archivist.

### **Third party use and disclosure of camera surveillance footage**

Compliance with IPP4(1)(b) requires agencies to take 'all reasonable steps' to prevent unauthorised use or disclosure of the personal information. Only Ipswich City Council had taken these steps, in the form of a statement in its forms restricting the use of the information, for example in its *CCTV Footage Release* form for release of camera footage to QPS:

***Restriction on use of disclosure.*** *In accordance with Information Privacy Principle 11(3) in Schedule 3 of the Information Privacy Act 2009 (Qld), Ipswich City Council requires that you must not use or disclose the information disclosed to you for a purpose other than for law enforcement or safety and welfare purposes.*

OIC noted that some of the agencies had well documented data security practices, for example Ipswich City Council.

Other agencies had little or no documentation, for example, James Cook University. Of particular note was the Townsville City Council who provided footage to QPS on nothing stronger than a belief that QPS would 'do the right thing with the information'. OIC notes that Council advised there had been two attempts to enter into Memoranda of Understanding with QPS over information exchange, with QPS declining to sign off on each Memorandum of Understanding. However, it does not appear that, in the absence of a general agreement, Townsville City Council took alternative reasonable steps to prevent unauthorised use or disclosure of the personal information, for example in a similar manner to the statement used by Ipswich City Council.

---

<sup>48</sup> For example - section 12.9.5 of the *General Retention and Disposal Schedule for Administrative Records (GRDS)*, states that surveillance video tapes used for monitoring security of premises which are not required for investigations, must be retained until the tape has been reviewed and verified by the agency that it has no further administrative use. Section 12.9.5 of the GRDS states surveillance video tapes used for monitoring security of premises which are required for investigations must be retained for one year after finalisation of investigative process or court proceedings and any appeals processes.

### 6.3 Analysis and Conclusion

Surveillance camera footage must be stored so that it is protected against loss, unauthorised access, use, modification, disclosure or any other misuse. Information Standard 18: Information Security (**IS18**) applies to Queensland Government departments<sup>49</sup> but IPP4 has a broader applicability.

In general, data security practices were well considered and adhered to strictly. There were exceptions.

The survey identified nine agencies that did not confirm that individuals could only access footage if authorised to do so, however, other data security measures were in place for seven of these nine agencies. Without further information, it would not be possible to draw a conclusion as to the actual level of risk associated with the absence of a control limiting access to camera surveillance footage to authorised persons. Nevertheless, these agencies are encouraged to consider adopting tighter data security controls over camera surveillance footage.

Given the widespread acceptance that extracted camera surveillance footage was a public record, unless its deletion was in accordance with a Retention and Disposal Schedule approved by the State Archivist, this deletion could constitute non-compliance with IPP4's injunction to protect data against loss or modification.

OIC considers that agencies would benefit from a general review of the retention and disposal of camera surveillance footage of all types. Agencies could then establish a Retention and Disposal Schedule that ensures the footage is kept and deleted in a considered and consistent manner that balances operational requirements including requests for access within a reasonable period.<sup>50</sup> OIC notes that, as discussed earlier, QSA has advised that it will consider re-issuing advice on this issue including the CCTV checklist from the Guideline to assist agencies. OIC considers that it is important for agencies to document their practices in policies and procedures, to ensure that the practices have been considered thoroughly and that sound operational practices are maintained as staff and systems change. All agencies would benefit from a review of the documentation of

<sup>49</sup> However, it remains an option for non-government agencies to adopt IS18 as practice.

<sup>50</sup> This information would also greatly benefit members of the public who may wish to access footage and may have no knowledge of the relatively short timeframe in which they would need to do this. See following chapter for more discussion on this issue.

their data security policies and procedures to ensure the written manuals are well considered, thorough and up-to-date.

#### **Recommendation Six**

It is recommended that:

Agencies ensure data security practices protect camera surveillance footage against loss, unauthorised access, disclosure, modification or other misuse and that these practices are described in documented policies and procedures.

## 7 Information Privacy Principle 5 – Individual can find footage

---

### Privacy requirements

**IPP5 Providing information about documents containing personal information.** An agency must take reasonable steps to ensure that a person can find out what personal information is held by the agency, the purpose for which the information is held and how an individual can obtain access to their personal information.

### **Information Privacy Principle 5 (IPP5) (equates to National Privacy Principle 5)**

Camera surveillance footage is part of the information holdings of an agency. IPP5 requires an agency to take reasonable steps to ensure that a person can find out whether or not footage is held, the purpose for holding the footage and how they can obtain access to footage containing their personal information. It should be easy for an individual to identify the owner of any publicly located camera and as readily, to apply for access to its captured footage.

Information concerning footage can be provided through a variety of means – as an addition to the camera's collection notice (see previous example of Western Downs Regional Council), as part of the agency's Privacy Plan/Privacy Policy or through a stand-alone resource.

In the interests of providing advice efficiently, the information should detail where the cameras are located, what information is captured through them and the currency of the footage.<sup>51</sup>

### Key findings

- Agencies generally have not considered or documented policies and procedures for advising individuals about camera surveillance footage held by the agency, or how an individual can access footage containing images of them.

---

<sup>51</sup> Commonly, footage that is not kept for evidentiary or other specific purposes is overwritten after a relatively short period of time.

## 7.1 Introduction

In order to test whether or not agencies take all reasonable steps to ensure that a person can find out what personal information is held by the agency, the purpose for which the information is held and how an individual can obtain access to their personal information, the agency survey asked about policies and procedures for accessing footage and providing it to others.<sup>52</sup>

The case studies also provided information as to agency practices in response to requests from individuals for footage concerning them.

OIC notes that the IP Act does not apply to covert surveillance and therefore IPP5 does not apply to such footage.

## 7.2 Findings

In the survey, only 9 agencies (20.9% of the 43 agencies actively informing the community) reported that they advised the public how to get access to camera surveillance footage. One of these was the Department of Communities.

In the detailed case studies, Ipswich City Council provided an exceptionally good list of personal information holdings in the Personal Information Digest No. 7. The Department of Communities produced a Privacy Guide listing personal information held by the department, including personal information recorded by camera surveillance systems. The other agencies did not provide advice about the personal information held as a result of camera surveillance. Townsville City Council had a privacy policy which made a general statement that Council would take all reasonable steps to assist an individual to discover and access personal information holdings. A search of websites for James Cook University and Logan City Council confirmed that even when agencies had privacy statements, these statements did not provide a general list of personal information holdings or specify personal information holdings collected through camera surveillance.

Only 19 agencies (44.2% of the 43 agencies actively informing the community) provided a notice of the surveillance in the immediate vicinity of the cameras. The site visits also illustrated the patchy provision of notices in the vicinity of the cameras to advise the community of the presence of the surveillance cameras.

---

<sup>52</sup> Questions 2.1 and 2.2 and 3.3.

### 7.3 Analysis and Conclusion

An agency having control of camera surveillance footage must take reasonable steps to ensure that a person can find out whether or not the footage is held, the purpose for holding the footage and how they can obtain access to footage containing their personal information.

Agencies generally demonstrated that they had not adopted the requirements of IPP5 in the management of the camera surveillance footage, with some exceptions.

This general dearth of information provided by agencies to the community about the agencies' personal information holdings limited the extent to which individuals would be able to exercise the rights afforded to them by the IP Act. If an individual does not know what personal information is held by an agency or even which agency holds their personal information, they are not in a position to access that information or seek to amend any inaccurate file records about them.

Agencies need to give immediate attention to the requirements of IPP5, and to establish a system so that individuals can find out the type of personal information captured by camera surveillance about them, the purposes for which this personal information is used and what they can do to obtain access to a record containing personal information about them.

As noted in section 3.3 of this Report, this requirement of the IP Act does not apply to covert surveillance footage.

#### Recommendation Seven

It is recommended that:

Agencies publish information about their holdings of camera surveillance footage including the currency of the footage, so that individuals can discover if there is any camera surveillance footage held by the agency which might contain images of them.

The lack of a notice in the vicinity of a camera to advise the community about the surveillance has a simple impact on an individual's ability to find out what personal information is held by an agency: they might not know which agency to approach in the first place. An individual cannot find out what footage is captured by an agency if they cannot find out which agency is operating a given surveillance camera. There might be limited

exceptions to this general principle where the ownership of the cameras is beyond doubt, for example, the operation of cameras in a detention centre.

OIC considers that a basic, threshold issue for the application of IPP5 is that agencies provide a notice with each of their cameras identifying themselves as the owner of the camera. An easy way to do this would be to put the agency's logo on the required collection notice located nearby to the camera installation or in the immediate vicinity of individual cameras.

An example of how this might be done has already been cited. The Western Downs Regional Council has an excellent collection notice adjacent to each camera, which contains the Council's logo and identifies that the camera is operated by the Council. Appendix 7 provides a copy of the notice.

### **Recommendation Eight**

It is recommended that:

Agencies provide publicly accessible information, preferably in the vicinity of each of the cameras they operate, informing the community of the camera's ownership and a point of contact for the relevant agency.

## 8 Information Privacy Principle 6 – Individual can access footage

---

### Privacy requirements

**IPP6 Access to documents containing personal information.** An individual must be able to access camera surveillance footage containing personal information about them.

### **Information Privacy Principle 6 (IPP6) (equates to National Privacy Principle 6)**

Under IPP6 an individual is able to access camera surveillance footage containing images of themselves. This capacity is not unfettered; if the agency has authority under an access law to deny access, IPP6 operates subject to this law. In practice, Chapter 3 of the IP Act is the default law governing access and accordingly, many agencies choose to process applications by individuals for access to footage through a formal IP Act access application.

To avoid unnecessary access applications, the individual should be able to ascertain prior to application whether, by reason of camera placement, technical issues or the simple passage of time, the agency does in fact have the required footage in its control or possession.

As mentioned in the discussion of data security and public records, OIC found agencies were routinely deleting camera surveillance footage on the basis that digital storage capacity was reached.

This practice has the important consequence that individuals might be unable to access personal information concerning them because it has been deleted. In many cases only the operating staff have knowledge of whether footage still exists. An example of useful information might be footage taken of a car accident, which might then be of value in an insurance claim. It has already been discussed that this type of information is not necessarily being managed in accordance with IPP4 and IPP5.

The deletion of this information might also be in conflict with adoption of IPP6. The insurance claim might take several months to be processed. If an individual cannot discover whether or not the footage might exist because there is not published list of information holdings (in contravention of IPP5), and the footage is deleted within a couple

### **Privacy requirements**

of weeks (possibly in contravention of IPP4), this important information might not be accessible (possibly in contravention of IPP6).

### **Key findings**

- Just over half of surveyed agencies that operated surveillance cameras informed the public that they conducted surveillance and of the ones that did, most did not inform the public they have rights to access the footage.
- Agencies reviewed in-depth had adopted an administrative process of blanket refusal.

## **8.1 Introduction**

In order to test whether or not agencies give individuals access to camera surveillance footage containing personal information about them if they ask for access, subject to access laws, the survey asked about agency practices and information provided to the community about individuals accessing footage.<sup>53</sup>

The case studies also provided information as to agency practices in response to requests from individuals for footage concerning them.

## **8.2 Findings**

In the survey, 43 agencies (56.6% of the 76 agencies operating surveillance cameras) stated that they actively informed the community about camera surveillance. Of these, only 9 agencies (20.9% of the 43 agencies actively informing the community) reported that they advised the public how to get access to camera surveillance footage.

## **Analysis and Conclusion**

In the case studies very few requests from individuals for access to camera surveillance footage were reported as being received, and it appeared in most cases agencies had

---

<sup>53</sup> Question 4.3.

refused access. Agency practices for dealing with requests should be examined against the requirements of legislation.

OIC acknowledges that the nature of camera surveillance can result in capture of personal information of a number of persons, not all of whom would necessarily be involved in a particular incident. As such requests for camera surveillance footage can require careful consideration of a number of competing interests on a case-by-case basis. For this reason, dealing with an access request under an administrative access scheme may not be appropriate.<sup>54</sup>

Members of the public can apply to access camera surveillance footage under the RTI and IP Acts. Camera surveillance footage is a 'document' of an agency and individuals have a right under the RTI and IP Acts to apply for access to footage.<sup>55</sup> While an applicant will usually have a practical reason for seeking access,<sup>56</sup> the motive of the applicant is irrelevant to the request. While some agencies may have genuinely-held concerns over the applicant's subsequent use of camera surveillance footage, the potential mischief by the applicant is an irrelevant factor in deciding whether disclosure would be contrary to the public interest.<sup>57</sup>

Some agencies considered that releasing camera surveillance footage to a third party breached the privacy of the individuals captured in the footage. This generalisation is a misreading of the privacy principles. Information Privacy Principle 11(1)(d) permits the disclosure of information to a third party if the disclosure is 'authorised or required under a law'. If after weighing competing public interests, a decision is made to release the personal information of a third party under the RTI or IP Act, disclosure to an applicant is then authorised under that Act for the purposes of IPP11.

If an agency had a policy or practice of denying an individual's access rights, it would be a breach of an agency's obligations under the RTI and IP Acts.

---

<sup>54</sup> OIC acknowledges the special case of footage released administratively to QPS where release is 'reasonably necessary' for a law enforcement function.

<sup>55</sup> OIC acknowledges that a right to apply for access does not necessarily equate to a right of access. Access applications must be decided on a case-by-case basis having regard to both the objects and requirements of the RTI and IP Acts.

<sup>56</sup> For example an individual whose car has been the victim of a 'hit and run' incident in a carpark operated by a government agency may wish to seek access to any available camera surveillance footage showing the incident in order for them to seek civil redress.

<sup>57</sup> Part 1(1) of Schedule 4 of the RTI Act.

Some refusals found in the course of this review were attributable to the agencies' deletion of camera surveillance footage after two to four weeks, which was usually done due to limited storage capacity within the system to retain footage beyond a couple of weeks. As stated earlier, OIC accepts that some agencies held different views about the status of this footage under the *Public Records Act 2002*.

As discussed previously, QSA recommends agencies adopt a risk based approach when determining the minimum retention periods for camera surveillance footage. If for example, footage is routinely deleted after two weeks as part of a managed cycle, documented in policies and procedures, the inability to provide footage (due to its deletion) would be justified.

However, OIC also found situations where the agency routinely deleted footage even when it had been extracted and passed on to a third party, for example, where footage had been extracted, copied and given to QPS. IPP11(2) requires a note of the disclosure to be included with the document, which would indicate the specific footage released itself at a minimum should be retained in such circumstances.

Where surveillance footage is accessed and/or copied (for example, when extracted camera surveillance footage is provided to the QPS for evidentiary purposes in a court proceeding), QSA stated a view the footage is a public record and as such, must be dealt with according to the General Retention and Disposal Schedule for Administrative Records<sup>58</sup> or alternatively, an agency / sector specific Retention and Disposal Schedule that has been approved by the State Archivist.

However, even where agencies had the footage, the general practice discovered by OIC was to refuse access to individuals seeking to view footage containing images of them.

This administrative practice was distinct from circumstances where agencies dealt with these requests as applications under the IP Act or RTI Act. This practice is potentially inconsistent with the IP Act.

---

<sup>58</sup> For example - section 12.9.5 of the *General Retention and Disposal Schedule for Administrative Records (GRDS)*, states that surveillance video tapes used for monitoring security of premises which are not required for investigations, must be retained until the tape has been reviewed and verified by the agency that it has no further administrative use. Section 12.9.5 of the GRDS states surveillance video tapes used for monitoring security of premises which are required for investigations must be retained for one year after finalisation of investigative process or court proceedings and any appeals processes.

The presumption adopted by agencies should be that individuals have a right to view footage containing their personal information, for example images of them, subject to the considerations outlined in the IP Act, for example, the agency is required under legislation to refuse to give the footage to the person for reasons relating to the privacy of other affected individuals. This should be documented in agency policy and procedures.

OIC is currently developing guidance material to assist agencies to comply with both their access application and privacy obligations.

#### **Recommendation Nine**

It is recommended that:

Agencies ensure they have policies and procedures in place which detail how individuals can obtain from an agency any camera surveillance footage which contains images of them, subject to exemptions prescribed in the *Information Privacy Act 2009* (Qld).

Further, the cumulative effect of IPP5 and IPP6 is that agencies should be more active in informing the community about the camera footage they hold and how it can be obtained.

#### **Recommendation Ten**

It is recommended that:

Agencies actively inform the community of the presence of camera surveillance systems, the rationale for their deployment, the privacy safeguards for the system and the mechanism by which the community can apply for access to the surveillance footage.

## 9 Information Privacy Principle 9 – Primary use of footage

---

### Privacy requirements

**IPP9 Use of personal information only for relevant purpose.** An agency must only use that part of camera surveillance footage which is directly relevant to the particular purpose for which it was collected.

### **Information Privacy Principle 9 (IPP9) (equates to National Privacy Principle 2)**

IPP9 states that if an agency contains a range of information concerning an individual, it must only use those portions of the information that are directly relevant to a given purpose.

In practice, an agency may have multiple footage of a particular person. For example, the individual may regularly pass by a street camera. If the individual is involved in a specific incident and that footage is required to be accessed by the agency, IPP9 requires that only the footage surrounding, or relevant to, the incident should be accessed and used.

### Key findings

- This was an area in which all case study agencies were compliant. Those agencies who regularly dealt with requests for footage by QPS actively took steps to only provide the footage relevant to the request. This could involve the agency staff member viewing several hours of footage just to extract a few relevant minutes.
- Case study agency practice had not been subject to corporate level review, except in the Ipswich City Council.

### 9.1 Introduction

The survey and case studies provided information as to agency usage of the footage.

## **9.2 Findings**

Agency comments in the survey provided some limited information as to agency use of camera surveillance. Two unique examples were the use of cameras for position of telescopes and to monitor water levels at river crossings to ensure roads had not been cut off. The most common reason for installing camera surveillance systems was property protection (89.5%), and this implies that surveyed agencies might monitor the cameras in real time as part of general building security.

The site visits suggested that the camera surveillance footage would rarely be accessed after an incident by the agency. It was more often the case that agency use of the footage was limited to accessing and reviewing the footage for the purpose of responding to QPS requests for information. A notable exception to this was in Ipswich City Council, where staff in the Safe City Program monitored the cameras in real time and contacted QPS to alert them to possible criminal activity before incidents occurred.

As discussed in this report, in most cases, it appears that agencies' responses to QPS requests for information after the fact was in the context of public safety initiatives and formal or informal partnerships or arrangements between agencies and the QPS.

Where QPS requested information, the standard practice observed in reviewed agencies was to view the section of footage in question to discover whether or not the relevant images had been captured. If the images were not there, the agencies generally communicated this to QPS, and agencies reported that QPS then would usually discontinue the request.

This was time consuming, with agency staff reporting that it could take several hours to identify whether or not a few minutes of footage was available and relevant, and if so, to extract that footage. OIC's observation was that in agencies reviewed operational practices were sound, but not well documented and generally had not been reviewed and approved at the corporate level.

## **9.3 Analysis and Conclusion**

An agency must only use that part of camera surveillance footage which is directly relevant to the particular purpose for which it was collected.

OIC found that this was occurring in practice, but that corporate level review had not occurred. Apart from ensuring that all corporate governance issues were addressed, particularly with respect to the application of the IP Act, corporate level review would enable monitoring of the level of agency resources being applied to review of footage on behalf of another agency (QPS), and amendment of the procedures if appropriate to regulate this activity.

#### **Recommendation Eleven**

It is recommended that:

Agencies review the way in which camera surveillance footage is scanned and material extracted in response to requests for copies of the footage, and ensure this process is demonstrably consistent with the privacy principles.

## 10 Information Privacy Principles 10 & 11 – Other use and disclosure

---

### Privacy requirements

**IPP10 Limits on use of personal information.** An agency might use camera surveillance footage for secondary purposes with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes.

**IPP11 Limits on disclosure.** Camera surveillance footage may be disclosed to other agencies with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes. Agencies might be expected to disclose surveillance camera footage to law enforcement agencies, for example, the Queensland Police Service (QPS).

### **Information Privacy Principle 10 (IPP10) (equates to National Privacy Principle 2)**

There are no IPP10 issues arising when an agency uses personal information for the purpose for which it obtained the information – termed the ‘primary use’. IPP10 operates to limit alternative or ‘secondary use’ of the personal information, for example, if camera surveillance was undertaken primarily to promote community safety, and then was also used for demographic profiling. IPP10 permits secondary usage where one (or more) of six circumstances apply. These circumstances include obtaining the consent of the individual concerned to the secondary use, legislative authority, law enforcement and health and safety considerations.

If the primary use is well-defined and articulated and the personal information is used exclusively in relation to that use, there will be no IPP10 conflict. IPP10 comes into play where an agency considers that the data store is useful for another, separate agency function. Sometimes the secondary use will not have been contemplated when the data was initially obtained. The secondary uses of data are often termed ‘function creep’ and this can be viewed suspiciously by the community.

The articulated reasons for camera surveillance are usually - security of persons and property. But camera surveillance is not necessarily restricted to these responsibilities.

## **Privacy requirements**

They can be used for such diverse functions as traffic monitoring and management, providing live (and therefore up-to-date) monitoring of river and creek levels and assistance in scheduling of maintenance (for example, graffiti clean-up).

It is accordingly important for agencies to clearly set out what the purpose of camera surveillance is. Lack of detailed information about primary purpose could lead to unwarranted community concerns about a potential IPP10 breach.

### **Information Privacy Principle 11 (IPP11) (equates to National Privacy Principle 2)**

Generally, personal information should not pass outside of an agency to anyone other than the person whose information is involved. As with secondary use, there are a number of circumstances under which the personal information can be disclosed to a third party including with consent, legislative authority, law enforcement and health and safety considerations.

Accordingly, an agency that 'owns' surveillance footage is limited in its capacity to provide it to someone else. There is the formal mechanism for a third party to apply for access to footage under the *Right to Information Act 2009*; provision of information in accordance with this legislation would be 'authorised or required under a law' – IPP11(1)(d).

While there is great flexibility for law enforcement under IPP11(1)(e), this permission requires that the disclosure be 'reasonably necessary'.<sup>59</sup> This test lies between that of administrative convenience and absolute necessity.

Before an agency releases camera surveillance footage to the Queensland Police Service (QPS), for example, for their law enforcement activities, the agency must satisfy the 'reasonable necessity test'. While this must be done on a case-by-case basis, agencies can use a standardised request form recording information supporting the 'case for necessity'. This information can include:

- the name and rank of the requesting police officer
- a counter-signature of a senior police officer
- the QPrime number (the QPS database reference number for the law enforcement

---

<sup>59</sup> This test also applies to secondary uses under IPPs10(1)(b) and (d) and a disclosure under IPP11(1)(c).

### **Privacy requirements**

activity for which the footage is requested)

- specific, limited description of footage sought
- brief description of the relevant criminal matter
- proposed use of the requested footage – for example, for evidentiary purposes in the prosecution of the offence
- the date of the request; and
- the date when the request is actioned and details of the actioning officer.<sup>60</sup>

IPP11(2) requires that when footage is given out for law enforcement purposes, a record of the disclosure must be included with the 'document' – the footage. This suggests that the agency should make a copy of the footage for its own records and include with that footage the QPS request form.

### **Key findings**

- A majority of government departments (77.8%) and local governments (54.3%) reported in the survey that they had disclosure arrangements with the QPS.
- Agencies have not generally considered or documented policies and procedures regulating the use and disclosure of camera surveillance footage.
- In particular, the case study agencies had partnered with QPS without formalising the arrangements to ensure disclosure of camera surveillance footage is managed in accordance with the IP Act.

## **10.1 Introduction**

In order to test whether or not agencies gave access only to relevant camera surveillance footage, the agency survey asked '*Does your agency have an administrative arrangement with any of the following entities concerning access to camera surveillance footage?*' and

---

<sup>60</sup> If there is a privacy challenge to the agency's provision of the footage to the QPS, the request form and the recollection of the relevant officer will provide the 'defence' to the challenge.

*‘Does this access occur according to a formal written agreement or in accordance with an established procedure?’<sup>61</sup>*

The case studies also provided information as to agency practices in response to requests for footage.

## **10.2 Findings**

Over one half (52.6%) of government agencies had an administrative arrangement with another agency concerning access to their camera surveillance footage: 42.1% had an administrative arrangement with the QPS, 11.8% with another government agency (excluding the QPS), and 6.6% with a non-government organisation.

A majority of government departments (77.8%) and local governments (54.3%) reported disclosure arrangements with the QPS.

Agencies with five or more policies/procedures for their camera surveillance systems had a higher incidence of administrative arrangements with the QPS (56.1%) and other government agencies (19.5%), than agencies with less than five policies/procedures (25.7% and 2.9% respectively).

Of the 40 agencies that had an administrative arrangement with another organisation, the majority (80.0%) allowed access to their camera surveillance footage according to a formal written agreement or in accordance with an established procedure. Local government councils (90.9%) appeared to be more likely than government departments (71.4%) and public authorities (63.6%) to have a formal written agreement or established procedure in place. Agencies that operated 11 – 100 cameras (86.7%) or more than 100 cameras (80.0%) also appeared more likely than agencies with 1 – 10 cameras (60.0%) to have a formal written agreement or established procedure in place.

This report does not reflect the full level of disclosure across surveyed agencies, as it did not identify informal practices of disclosure.

OIC examined arrangements through the case studies. Ipswich City Council and Logan City Council had formal written agreements for disclosing information to another agency. Ipswich City Council did not provide a Memorandum of Understanding, but had a system described in a detailed manual supported by standard forms for QPS to request and obtain camera surveillance footage. Logan City Council had a formal agreement with Queensland Rail

---

<sup>61</sup> Questions 6.1 and 6.2.

which made explicit mention of privacy, and a formal agreement with QPS which mentioned the need for confidentiality but did not explicitly mention the privacy principles.

### 10.3 Analysis and Conclusion

An agency might use camera surveillance footage for secondary purposes with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes.

A recent example of secondary use was a pilot program of Ipswich City Council which involved the authorised staff monitoring the camera surveillance system going through archival footage to identify parking infringers. As this action could not be associated with the stated purposes of public safety or property protection, the use of camera surveillance footage would have to be justified by one of the exemptions available in IPP10.<sup>62</sup> Ipswich City Council discontinued this practice at the conclusion of the pilot.

#### Recommendation Twelve

It is recommended that:

Agencies ensure policies and procedures are in place for use and disclosure of personal information that ensure that personal information is used for secondary purposes or disclosed only as provided for in the *Information Privacy Act 2009* (Qld), for example, with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes.

Camera surveillance footage may be disclosed to other agencies as provided for in the IP Act, for example, with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes. Agencies would usually cooperate with requests from law enforcement agencies, for example, QPS for access to surveillance camera footage.

This review found that the most likely entity to which agencies disclosed surveillance footage was QPS for use in law enforcement activities.

<sup>62</sup> Potentially the exemption in IPP10(1)(d)(i) could apply to this use.

Agencies with larger installations or with more than five policies were more likely to have a disclosure arrangement with the QPS. This might be an indicator of the tendency of these agencies to formalise and document procedures. The in-depth review suggested that more agencies would be disclosing footage to QPS informally, without an administrative arrangement. By and large, these disclosures could be expected to fall within the legislative exemptions which permit disclosure to third parties for law enforcement. Importantly, though, in order for agencies to comply with their obligation under IPP11 they must satisfy themselves that their disclosure is 'reasonably necessary' for a law enforcement purpose.

The case studies found even where an administrative arrangement did not exist, agencies were requiring QPS to complete a request form to obtain footage, and this form generally prompted for some of the factors that would satisfy the agency of the necessity for QPS to obtain the footage in pursuit of a law enforcement activity. The best example of this form was used by Ipswich City Council. A copy of this form is provided in Appendix 6, to assist agencies in developing a form which addresses the requirements of IPP11(1)(e) in full.

OIC considered the approach of the case study agencies was commendable, but could be improved by a review of all relevant documents to ensure the privacy principles were explicitly addressed.

### **Recommendation Thirteen**

It is recommended that:

Agencies develop administrative arrangements for disclosure of information where this is usual practice, for example, a Memorandum of Understanding with the Queensland Police Service, and adopt a standardised request form which ensures disclosure of camera surveillance footage is in accordance with the privacy principles.

## 11 Information Privacy Principles – Contractors

---

### **Privacy requirements**

In the main, the privacy principles only apply to Queensland government agencies. They do not apply to private sector firms, community sector organisations or individuals. The one potential exception is where the government agency outsources its functions to a non-government entity and that arrangement involves the flow of personal information.

For contracts and other arrangements of this nature entered into after 1 July 2009 (1 July 2010 for local government), the agency is obligated under Chapter 2, Part 4 of the IP Act to bind the non-government entity to compliance with the obligations under the relevant privacy principles. If so bound, the entity assumes the same obligations as the contracting agency.

The benefit to the agency is that once bound, the entity assumes all liabilities for any subsequent privacy shortfalls.<sup>63</sup> If the agency fails to take all reasonable steps then it retains liability for privacy shortfalls of the contracted entity.

### **Key findings**

- Agencies have generally not had to consider binding private service providers at this time, and so these issues have received only sporadic attention.

### **11.1 Introduction**

In order to test whether or not agencies bound contracted service providers to the privacy principles, the agency survey asked *'Is your agency's camera surveillance system operated in part or fully by a private sector contractor?'* and a series of questions to establish the date that any contracts commenced and the terms of the contracts with respect to the IPPs.<sup>64</sup>

The case studies also provided information as to agency dealings with contracted service providers.

---

<sup>63</sup> Outsourcing is a significant privacy vulnerability for agencies. The 2010 Annual Study 'Australian Cost of a Data Breach' by the Ponemon Institute found that 37% of privacy breaches involved outsourced data to third parties – up from 31% in 2009.

<sup>64</sup> Questions 7.1 to 7.4.

## 11.2 Findings, Analysis and Conclusion

Over one quarter of agencies (27.6% of agencies) that operated camera surveillance systems indicated that the systems were operated fully or in part by a private contractor. Six agencies entered into these contracts after the IP Act became applicable to their agency, and five of those six agencies had a contract which bound the contractor to compliance with the IP Act. The sixth agency reported they were developing a Memorandum of Understanding with the service provider.

The review found that the nature of these contracts tended to be about the use of a private sector security firm to administer the system. For example, two of the agencies reviewed in depth had employed a security firm to monitor the camera surveillance footage. Of these two agencies, one reported binding the private service provider to the privacy principles and the other had entered into their contract prior to the commencement of the IP Act.

These findings demonstrated that the issue has not yet arisen for most agencies, and where it has, the agencies have been reasonably focussed on ensuring the service providers were bound to the privacy principles.

In practice, it will not be an onerous obligation for service providers, for example security firms. A number of firms will be large enough and sufficiently well-established that they already work within the privacy obligations in the Commonwealth's *Privacy Act 1988*.<sup>65</sup> However, agencies should not rely on the entity's Commonwealth *Privacy Act 1988* obligations in its arrangements, as the Commonwealth law has no application to state contracts.

Agencies are also encouraged to consider reviewing existing contracts with private security contractors to ensure that any service contracts encompass a requirement to comply with the privacy principles.

### Recommendation Fourteen

It is recommended that:

Agencies review contracts with private security contractors to ensure contracts bind the contractors to compliance with the privacy principles.

<sup>65</sup> An organisation that has an annual turnover of more than \$3 million can be covered by the National Privacy Principles in the Commonwealth *Privacy Act 1988*.

## 12 Information Privacy Principles – Overseas transfer of information

---

### Privacy requirements

Section 33 of the IP Act is crafted to ensure that when personal information is transferred overseas, the information is subject to similar protections to those in Queensland. In the alternative, there must be clear legislative authority for the transfer, there must be a serious health or safety threat or the individual themselves must consent to the information being transferred.

This protection covers all online activity from web-sites, cloud services, off-shore data storage and processing and the online tools such as survey applications.

The obligations in section 33 will not ordinarily arise in the case of camera surveillance footage as it is rarely put online<sup>66</sup> or otherwise transferred overseas. Consideration as to the applicability of this section would need to occur if the agency used the cloud<sup>67</sup> or other off-shore facilities for storage of the footage.

Section 33 is not enlivened if an agency electronically transmits footage within Australia.

### Key findings

- Agencies have generally not had to consider regulating the transfer of camera surveillance footage overseas (for example by transmitting footage over the internet), and so these issues have received little attention.

### 12.1 Introduction

In order to test whether or not agencies protected information passed overseas, the agency survey asked *'Is the camera footage available on the internet?'* and *'Is the camera footage stored offshore, eg. in the cloud, or with a contractor or service provider located outside Australia?'* and *'Is the camera footage passed outside Australia by any other means?'* and *'Does your agency have a policy and/or procedure to ensure compliance with the privacy*

---

<sup>66</sup> There are exceptions, most notably highway traffic cams. However, these cameras arguably do not capture personal information as defined in section 12 of the IP Act.

<sup>67</sup> Defined in Appendix 1.

*obligations surrounding transfer of personal information outside Australia (section 33 of the IP Act)?*.<sup>68</sup>

The case studies also provided information as to protection of personal information transferred overseas.

## **12.2 Findings, Analysis and Conclusion**

Five agencies reported that they transferred or stored camera surveillance information overseas. Two of these had policies and procedures covering privacy obligations. In at least two instances, the circumstances of placing the footage on the internet were unique and unobjectionable, for example, the use of a webcam to check whether or not the water level of a creek had risen so as to cut off the road, or the use of camera footage online to check the positioning of remotely based astronomical telescopes.

In these circumstances, this is a low risk concern.

OIC considers that the issue of handling information transferred overseas should be incorporated into any privacy review of camera surveillance policies and procedures.

### **Recommendation Fifteen**

It is recommended that:

Agencies develop policies and procedures to ensure that any camera surveillance footage transferred overseas, for example placed on the internet, is done within a clear legislative authority.

---

<sup>68</sup> Question 7.1 to 7.4.

## 13 Conclusion

---

Agencies reported using in excess of 20,000 surveillance cameras to promote public safety, maintain good order and prevent property crimes such as theft and vandalism. Agencies felt that positive media reports about camera surveillance increased confidence in the community about public safety. By and large, the cameras being operated by Queensland government agencies were being operated by people who were mindful of privacy issues. This was primarily due to the efforts of operational staff, who have applied common sense to the development and operation of the systems.

Nevertheless, the over arching finding of this review is that Queensland public sector agencies have further work to do in identifying, managing and reducing existing privacy risks to the community associated with agency use of camera surveillance footage. This is particularly critical given the increasing use of camera surveillance by Queensland government agencies and the need to satisfy higher community expectations regarding the management of such privacy risks.

Generally, executive management have not adequately turned their minds to the governance questions about camera surveillance: questions of the reason for having camera surveillance; the scope and boundaries of its use; its effectiveness, as demonstrated by hard evidence; how the camera footage should be used, disclosed, kept or destroyed; and most relevantly for this review, the privacy rights of individuals. The disconnection between corporate governance and local operations has resulted in a range of privacy impacts, including concerning signs that legislative non-compliance is occurring in some respects.

Widespread camera surveillance has costs, not least in the area of privacy. When a surveillance system is poorly managed, public concerns can arise about the advent of a 'Big Brother' culture, which includes a range of concerns about unnecessary surveillance, poorly targeted surveillance, costs outweighing benefits, information being gathered about individuals for secret or inappropriate purposes, lack of access and accountability in government and generally that the system is degraded and ineffective. These concerns are particularly liable to arise if the camera system fails to deliver on advertised benefits such as the prevention of crime.

Privacy does not necessarily equate to secrecy. The essence of privacy - that '*no-one should be subjected to arbitrary interference with [their] privacy...*'<sup>69</sup> – implicitly incorporates a measured use of personal information for legitimate purposes.

The privacy principles in the IP Act are important in helping agencies establish the balance between the capture of personal information and the provision of beneficial services. The balancing of privacy protections with legitimate use is in part achieved by compliance with the privacy principles in the IP Act. The privacy principles cover off issues such as:

- ensuring a surveillance program does not unnecessarily impinge upon individual privacy
- informing the community about the camera surveillance strategy and its operations so that the community can actively participate in and benefit from its proper operation and in protecting their own privacy;<sup>70</sup> and
- managing the flow and the security of information generated by the camera surveillance so that the potential for misuse or abuse of the information is removed or minimised.

Camera surveillance systems are likely to continue to expand. It is accordingly important that privacy considerations be incorporated into every aspect of their operation from planning to deployment to decommissioning and that this incorporation be adequately communicated to the community.

These issues could be readily resolved by agencies taking these steps:

- clear identification of the objectives of camera surveillance ensuring the objectives are aligned with the functions of the agency
- before introduction or expansion of use, conduct of an evidence based cost/benefit analysis of camera surveillance for the purpose and context, including privacy harms associated with the type of equipment being used and the location
- review at the corporate level of the overall policies and procedures for the development and operation of camera surveillance systems

---

<sup>69</sup> Article 12 - 1948 Universal Declaration of Human Rights and Article 17, International Covenant on Civil and Political Rights, 1966.

<sup>70</sup> For example, if an individual knew that a particular walkway was actively monitored by security staff, they could more preferentially use that walkway.

- documentation of policies and procedures for the operation and development of camera surveillance systems
- implementation of systems to ensure operational take-up of policies and procedures for the camera surveillance system; and
- evaluation as to whether camera surveillance has achieved stated objectives.



## **APPENDICES**



## Appendix 1 – Acronyms

---

CCTV	Closed-Circuit Television
CCYPCG	Commission for Children, Young People and the Child Guardian
Cloud	Delivering hosted computer services over the internet
CMC	Crime and Misconduct Commission
CPTED	Crime Prevention Through Environmental Design
CSSC	Child Safety Service Centre
FOI	Freedom of Information
FOI Act	<i>Freedom of Information Act 1992 (Qld)</i>
ICT	Information and Communications Technology
IP	Information Privacy
IP Act	<i>Information Privacy Act 2009 (Qld)</i>
IPP	Information Privacy Principle
IS42	Information Standard 42
IS42A	Information Standard 42A
NPP	National Privacy Principle
OESR	Office of Economic and Statistical Research
OIC	Office of the Information Commissioner
OLGR	Office of Liquor and Gaming Regulation
PTZ	Pan Tilt Zoom Cameras
QPrime	Queensland Police Records and Information Management Exchange – the Queensland Police Service's database to manage information about law enforcement activities.
QPS	Queensland Police Service
QSA	Queensland State Archives
RTI	Right to Information
RTI Act	<i>Right to Information Act 2009 (Qld)</i>



## **Appendix 2 – The Information Privacy Principles**

---

### **1 IPP 1—Collection of personal information (lawful and fair)**

- (1) An agency must not collect personal information for inclusion in a document or generally available publication unless—
  - (a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and
  - (b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.
- (2) An agency must not collect personal information in a way that is unfair or unlawful.

### **2 IPP 2—Collection of personal information (requested from individual)**

- (1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.
- (2) However, this section applies only if the agency asks the individual the subject of the personal information for either—
  - (a) the personal information; or
  - (b) information of a type that would include the personal information.
- (3) The agency must take all reasonable steps to ensure that the individual is generally aware of—
  - (a) the purpose of the collection; and
  - (b) if the collection of the personal information is authorised or required under a law—
    - (i) the fact that the collection of the information is authorised or required under a law; and
    - (ii) the law authorising or requiring the collection; and
  - (c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the first entity)—the identity of the first entity; and
  - (d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the second entity)—the identity of the second entity.
- (4) The agency must take the reasonable steps required under subsection (3)—
  - (a) if practicable—before the personal information is collected; or
  - (b) otherwise—as soon as practicable after the personal information is collected.

- (5) However, the agency is not required to act under subsection (3) if—
  - (a) the personal information is collected in the context of the delivery of an emergency service; and

*Example —*

personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service

- (b) the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and
- (c) the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

### **3 IPP 3—Collection of personal information (relevance etc.)**

- (1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.
- (2) However, this section applies to personal information only if the agency asks for the personal information from any person.
- (3) The agency must take all reasonable steps to ensure that—
  - (a) the personal information collected is—
    - (i) relevant to the purpose for which it is collected; and
    - (ii) complete and up to date; and
  - (b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

### **4 IPP 4—Storage and security of personal information**

- (1) An agency having control of a document containing personal information must ensure that—
  - (a) the document is protected against—
    - (i) loss; and
    - (ii) unauthorised access, use, modification or disclosure; and
    - (iii) any other misuse; and
  - (b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.

- (2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

#### **5 IPP 5—Providing information about documents containing personal information**

- (1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out—
  - (a) whether the agency has control of any documents containing personal information; and
  - (b) the type of personal information contained in the documents; and
  - (c) the main purposes for which personal information included in the documents is used; and
  - (d) what an individual should do to obtain access to a document containing personal information about the individual.
- (2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

#### **6 IPP 6—Access to documents containing personal information**

- (1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.
- (2) An agency is not required to give an individual access to a document under subsection (1) if—
  - (a) the agency is authorised or required under an access law to refuse to give the access to the individual; or
  - (b) the document is expressly excluded from the operation of an access law.

#### **7 IPP 7—Amendment of documents containing personal information**

- (1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information—
  - (a) is accurate; and
  - (b) having regard to the purpose for which it was collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.
- (2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.

- (3) Subsection (4) applies if—
  - (a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and
  - (b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).
- (4) The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

#### **8 IPP 8—Checking of accuracy etc. of personal information before use by agency**

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, complete and up to date.

#### **9 IPP 9—Use of personal information only for relevant purpose**

- (1) This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.
- (2) The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

#### **10 IPP 10—Limits on use of personal information**

- (1) An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless—
  - (a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the other purpose; or
  - (b) the agency is satisfied on reasonable grounds that use of the information for the other purpose 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
  - (c) use of the information for the other purpose is authorised or required under a law; or
  - (d) the agency is satisfied on reasonable grounds that use of the information for the other purpose 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
- (e) the other purpose is directly related to the purpose for which the information was obtained; or

*Examples for paragraph (e) —*

- 1 An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.
- 2 An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivering improvements to the core services.
- (f) all of the following apply—
  - (i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest;
  - (ii) the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information;
  - (iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

- (2) If the agency uses the personal information under subsection (1)(d), the agency must include with the document a note of the use.

## **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—
  - (i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
  - (ii) the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;
  - (iii) 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.
- (3) If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not use or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.
- (4) The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that—
  - (a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and
  - (b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and
  - (c) the individual has not made a request mentioned in paragraph (b); and
  - (d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and
  - (e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically.



## **Appendix 3 – Terms of Reference**

---

### **Terms of Reference**

#### **Review of camera surveillance use by Queensland government agencies and information privacy**

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

To examine and report on Queensland government agencies use of camera surveillance (for example Closed-Circuit Television (CCTV) cameras) to:

- a. establish whether agencies comply with the prescribed requirements of the *Information Privacy Act 2009* (Qld) (IP Act)
- b. identify areas of good practice
- c. make recommendations to improve compliance with the IP Act.

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

The Information Commissioner, under section 135 of the IP Act can conduct reviews into personal information handling practices and audits of compliance with the information privacy principles (IPP).

The review will examine Queensland government agencies' use of camera surveillance with respect to information handling practices and compliance with the information privacy principles under the IP Act. This will include an examination of:-

- a. Agency governance (leadership, governance mechanisms, information management policies, procedures, delegations and roles and responsibilities of key personnel and training)
- b. Accountability and performance monitoring systems
- c. Compliance with legislatively based requirements for:
  - i. Collecting personal information lawfully and fairly (IPP 1)
  - ii. Only collecting personal information that is relevant and which is not an unreasonable intrusion into their personal affairs (IPP 3)
  - iii. Ensuring the security of the information collected (IPP 4)
  - iv. Ensuring that people can find out about personal information collected (IPP 5)
  - v. Ensuring individuals can access a document which contains their personal information on request (IPP 6)
  - vi. Using the personal information for a particular purpose or under a specific exemption (IPPs 9 and 10); and
  - vii. Disclosing the personal information only as permitted by law (IPP 11).

- d. The extent to which the community is informed on the purpose for and the uses of each camera used for surveillance; and
- e. The extent to which the agency engages with the community about the implementation and use of camera surveillance and the handling of information gathered through camera surveillance.

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

The review is based on an assessment of the performance of the agency against the requirements in the IP Act, and any subordinate guidelines or instruments made under the legislation.

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 tests whether or not the agency has complied with that requirement.

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.

These requirements are summarised in an OIC publication titled *Right to Information and Information Privacy Agency Self Assessment Tool* which details all of the legislative obligations contained in the *Right to information Act 2009* (Qld) and the IP Act. This is available on the OIC website at <http://www.oic.qld.gov.au/files/Agency%20Self%20Assessment%20Tool.doc> and has been previously sent to agencies.

### **4. Assessment Process**

The Manager, Performance Monitoring and Reporting, the Principal Privacy Officer and the Senior Performance, Monitoring & Reporting Officer will conduct the review.

Evidence may be gathered through the following processes:

- a. Discussions with relevant staff and management
- b. Observation of personal information handling practices
- c. Examination of agency website and intranet
- d. A survey of agency camera surveillance implementation and use
- e. In-depth compliance review of a sample of agencies, including site inspections
- f. Review of statistical records/reporting; and
- g. Consultation with stakeholders in government and the community to discuss issues for the use of camera surveillance cameras by government agencies.

### **5. Reporting**

The report will present findings and make recommendations to improve agency compliance with the obligations in the IP Act and to identify areas of good practice.

Survey results will be included in the report in aggregate form, represented by total respondent agencies or by sector (for example, local government agencies). This

means that where consideration of an agency in this review is limited to their participation in the survey, that agency will not be identified in the report.

Issues identified during the review regarding agency management of camera surveillance systems will be raised progressively during the review with each agency as appropriate. If necessary, OIC will provide a briefing to management within an agency before drafting the review report.

The draft review report will incorporate issues identified during the review and any agency comments. Agencies subject to an in depth compliance review will be given an opportunity to comment formally on issues, findings and recommendations in the draft report to the extent that they specifically relate to their agency.

This final report, together with the agencies' formal response to recommendations, will be submitted to the Speaker for tabling in the Legislative Assembly.

## **6. Administrative Matters**

At this stage, it is envisaged that the review will commence in October 2011 and be finalised by January 2012. The exit meetings and report drafting should be concluded by the end of April 2012, assuming no intervening circumstances.



## Appendix 4 – Office of Economic and Statistical Research Survey Report

---



**Use of Camera Surveillance (CCTV)  
Survey 2011-12**

**Survey Report**

*prepared for*

**Office of the Information Commissioner**

Office of Economic and Statistical Research  
Level 8, 33 Charlotte Street  
Brisbane QLD 4000  
Ph: (07) 3224 5326  
<http://www.oesr.qld.gov.au>

**1/03/2012  
Final Version**

This report is for the exclusive use of Office of the Information Commissioner without restriction.

All data and information in this document are believed to be accurate and have come from sources believed to be reliable. However, the Office of Economic and Statistical Research, Queensland Treasury does not guarantee or represent that the data and information are accurate, up to date or complete, and disclaims liability for all claims, losses, damages or costs of whatever nature and howsoever occurring, arising as a result of relying on the data and information, regardless of the form of action, whether in contract, tort (including negligence), breach of statutory duty or otherwise.

© The State of Queensland (Queensland Treasury) (2012)

ii

## Contents

1	EXECUTIVE SUMMARY .....	1
2	INTRODUCTION .....	4
2.1	Background.....	4
2.2	Objectives.....	4
3	METHODOLOGY .....	5
3.1	Survey instrument design .....	5
3.2	Survey frame .....	5
3.3	Data collection method.....	5
3.4	Final status and scope of agencies on frame .....	6
3.5	Survey response rate.....	6
3.6	Respondent inquiries .....	8
3.7	Data cleaning.....	8
4	SURVEY RESULTS .....	9
4.1	Presentation and interpretation .....	9
4.2	Comparison groups .....	9
4.3	Surveillance camera deployment.....	10
4.4	Policies and procedures to administer surveillance camera systems .....	12
4.5	Purposes for implementation and use of surveillance camera systems .....	15
4.6	Notifying the community about camera surveillance.....	16
4.7	Data storage and security of camera surveillance footage.....	18
4.8	Disclosure of camera surveillance footage.....	20
4.9	Private contractors for surveillance camera systems.....	21
4.10	Passing camera surveillance footage outside Australia.....	23
5	GLOSSARY .....	25
6	APPENDICES .....	26
	Appendix 1 – Survey instrument .....	26
	Appendix 2 – List of non-responding agencies.....	39
	Appendix 3 – Output tables .....	41
	Appendix 4 – Considerations for future projects .....	51

## List of tables

Table 1	Number of government agencies on frame, by agency type .....	5
Table 2	Final status of government agencies on frame .....	6
Table 3	Final status of in-scope government agencies .....	6
Table 4	Response rate by agency type .....	7
Table 5	Whether government agencies operated surveillance cameras .....	10
Table 6	Total number of cameras operated, by agency type .....	10
Table 7	Number of cameras operated by government agencies .....	11
Table 8	Monitoring purpose of cameras .....	11
Table 9	Whether footage of private property captured through use of camera surveillance .....	12
Table 10	Number of documented policies/procedures for surveillance camera systems .....	13
Table 11	Whether training provided to staff in surveillance camera system policies and procedures .....	13
Table 12	Status of documented policies/procedures for camera surveillance systems .....	14
Table 13	Reasons for installing camera surveillance systems .....	15
Table 14	Information and evidence that supported introduction of camera surveillance systems .....	16
Table 15	Whether community is actively informed about surveillance .....	17
Table 16	How information is provided when notifying community about camera surveillance .....	17
Table 17	Types of information provided to community about camera surveillance .....	18
Table 18	Where surveillance camera footage is stored .....	19
Table 19	How access to surveillance camera footage is managed .....	19
Table 20	Type of organisations with administrative arrangements concerning access to camera surveillance footage .....	20
Table 21	Whether access to footage by other organisations occurs according to a formal written agreement or established procedure .....	21
Table 22	Whether camera surveillance systems operated in part or fully by private sector contractors .....	21
Table 23	Date that contracts with private sector contractors were entered into .....	22
Table 24	Items covered in contracts with private sector contractors .....	22
Table 25	Whether contractors were bound to compliance with privacy principles in the IP Act .....	23
Table 26	Whether camera surveillance footage was passed outside Australia .....	23
Table A3a	Reasons for installing camera surveillance systems, by agency type .....	41
Table A3b	Reasons for installing camera surveillance systems, by number of cameras .....	42
Table A3c	Reasons for installing camera surveillance systems, by policy implementation .....	43
Table A3d	Information and evidence that supported introduction of camera surveillance systems, by agency type .....	44
Table A3e	Information and evidence that supported introduction of camera surveillance systems, by number of cameras .....	45
Table A3f	Information and evidence that supported introduction of camera surveillance systems, by policy implementation .....	46
Table A3g	Overlap between how information is provided when notifying community about camera surveillance .....	47
Table A3h	How access to surveillance camera footage is managed, by agency type .....	48
Table A3i	How access to surveillance camera footage is managed, by number of cameras .....	49
Table A3j	How access to surveillance camera footage is managed, by policy implementation .....	50

**Abbreviations**

The following abbreviations and symbols are used in this report:

IP	Information Privacy
OESR	Office of Economic and Statistical Research
OIC	Office of the Information Commissioner

# **1 EXECUTIVE SUMMARY**

## **Background and methodology**

The Use of Camera Surveillance Survey 2011-12 (referred to in this report as the CCTV Survey) was conducted by the Office of Economic and Statistical Research (OESR) on behalf of the Office of the Information Commissioner (OIC). The survey was conducted by web and ran from 15 November 2011 to 30 January 2012. A total of 122 completed questionnaires were received, resulting in a response rate of 69.3%.

The objective of the CCTV Survey was to assist the OIC to fulfil its legislative requirements to monitor and report on the extent to which agencies are complying with the *Information Privacy Act 2009* (IP Act) in their implementation and use of closed-circuit television. Under Section 135 of the IP Act, the Information Commissioner can conduct reviews into personal information handling practices of agencies and conduct compliance audits to assess agency compliance with the privacy principles.

The survey results identified the purposes for which camera surveillance systems have been installed and provided an indication of how well the general administration of the system complies with the privacy principles.

## **Key results**

### **Surveillance camera deployment**

Of the 122 Queensland government agencies that responded, 62.3% operated surveillance cameras. Of the 20,310 cameras in operation, 71.2% were used for the purpose of monitoring in or around government buildings and 13.4% for monitoring pedestrian traffic.

Government departments (75.0%) and local government councils (76.1%) appeared to be more likely than public authorities (50.0%) to operate surveillance cameras. The majority (88.9%) of government departments operated more than 100 cameras, while local government councils (77.1%) and public authorities (71.9%) each tended to operate 100 cameras or less.

Of the 76 agencies that operated surveillance cameras, approximately one third (32.9%) captured footage of private property through their use of camera surveillance. Local government councils (45.7%) and agencies with over 100 cameras (44.0%) appeared to be the most likely to capture footage of private property.

### **Policies and procedures to administer surveillance camera systems**

Over one half of agencies that operated surveillance cameras had a documented policy and/or procedure for:

- providing surveillance camera footage to others (59.2%);
- accessing surveillance camera footage (57.9%);
- instructions for staff operating the surveillance camera system (56.6%); and
- retention and disposal of surveillance camera footage (51.3%).

However, less than one third (31.6%) of government agencies provided training to staff in policies and procedures. Agencies with five or more documented policies/procedures for their camera surveillance systems (51.2%) appeared much more likely than agencies with less than 5 policies/procedures (8.6%) to provide their staff with training.

#### Purposes for implementation and use of surveillance camera systems

The most common reason for installing camera surveillance systems was property protection (89.5%), followed by crime prevention (77.6%), public safety (76.3%), crime investigation and enforcement (64.5%), and improving agency capacity to respond to issues (51.3%). The most common forms of information or evidence that supported the introduction of camera surveillance systems was research into their effectiveness (40.8%) and evaluations of existing systems (36.8%).

#### Notifying the community about camera surveillance

Over one half (56.6%) of government agencies that operated surveillance cameras actively informed the community about the surveillance.

- Over two thirds (67.4%) of these agencies notified the community through a notice in the general area where cameras were used, 44.2% by a notice in the immediate vicinity of each camera, 34.9% on individual request, 30.2% in a publicly accessible document, and 16.3% through media releases.
- Approximately three in five (62.8%) provided information about the purpose of the surveillance system generally, 27.9% provided information about whether it is the agency's usual practice to disclose footage to any other individual, agency, or organisation, and 20.9% on how to get access to the footage.

#### Data storage, security and disclosure of camera surveillance footage

The majority of agencies (88.2%) stored their surveillance camera footage in their own agency facilities, and almost all (96.1%) managed access to their camera footage.

Over one half (52.6%) of government agencies had an administrative arrangement with another agency concerning access to their camera surveillance footage.

- 42.1% had an administrative arrangement with the Queensland Police Service;
- 11.8% with another government agency (excluding Queensland Police Service); and
- 6.6% with a non-government organisation.

Of the 40 agencies that had an administrative arrangement with another organisation, the majority (80.0%) allowed access to their camera surveillance footage according to a formal written agreement or in accordance with an established procedure.

Very few agencies (5.3%) passed their camera footage outside of Australia. Of the four agencies that did, two had a policy and/or procedure to ensure compliance with the privacy obligations surrounding transfer of personal information outside Australia.

#### Private contractors for surveillance camera systems

Over one quarter (27.6%) of agencies that operated camera surveillance systems indicated that their surveillance systems were operated in part or fully by a private sector contractor.

Of these, 61.9% entered into a contract before 30 June 2009. Two thirds (66.7%) had contracts which covered access to the footage and the safety and security of the footage, 61.9% covered the disclosure of footage to third parties, and over one half (52.4%) covered the secondary use of footage and the retention and disposal of footage.

Five out of the six agencies (83.3%) whose contract was entered into on or after 1 July 2009 had a contract which bound the contractor to compliance with the privacy principles in the IP Act.

#### General trends

Government agencies that were classified as departments, operated more than 100 cameras, or had five or more policies/procedures for their camera surveillance systems, tended to be more likely to:

- have documented policies and/or procedures for their camera surveillance systems;
- provide staff with training in policies and procedures for their camera surveillance systems;
- use information and evidence to support the introduction of their camera surveillance systems;
- actively inform the community about their camera surveillance;
- implement formal management procedures for their surveillance camera footage;
- have an administrative arrangement with the Queensland Police Service concerning access to their camera surveillance footage; and
- have a private sector contractor operate their camera surveillance systems.

## **2 INTRODUCTION**

The CCTV Survey 2011-12 was conducted by OESR on behalf of OIC. The survey ran from 15 November 2011 to 30 January 2012.

### **2.1 Background**

The IP Act provides safeguards for the handling of personal information in the public sector environment, and allows access to and amendment of personal information.

Under Section 135 of the IP Act, the Information Commissioner can conduct reviews into personal information handling practices of agencies and conduct compliance audits to assess agency compliance with the privacy principles.

Queensland State Archive's *Guideline for Managing Closed Circuit Television Records* provides further information about the management of surveillance footage as public records, in accordance with the requirements of the IP Act.

### **2.2 Objectives**

The objective of the CCTV Survey was to assist the OIC to fulfil its legislative requirements to monitor and report on the extent to which agencies are complying with the IP Act in their implementation and use of closed-circuit television.

The survey results identified the purposes for which camera surveillance systems have been installed and provided an indication of how well the general administration of the system complies with the privacy principles.

### 3 METHODOLOGY

#### 3.1 Survey instrument design

Questions were developed by OIC, with technical advice offered by statisticians in OESR. The questionnaire is included in Appendix 1.

#### 3.2 Survey frame

The CCTV Survey targeted public authorities which are defined in the Right to Information legislation as being established for a public purpose by, or under, an Act. A list of 179 Queensland government departments and agencies was compiled by OIC, and comprised the survey frame.

Table 1 describes the percentage of government agencies on the survey frame by agency type. Of the 179 Queensland government agencies on the frame, 74 (41.3%) were local government councils, 65 (36.3%) were statutory authorities and advisory boards, 13 (7.3%) were government departments, and 13 (7.3%) were Queensland Health agencies. The remaining 14 government agencies (7.8%) were a variety of universities, TAFEs and other agencies.

**Table 1** Number of government agencies on frame, by agency type

	Frequency	Percentage (%)
Departments	13	7.3
Local government councils	74	41.3
Medical research institutes	1	0.6
Queensland Health agencies	13	7.3
Statutory authorities and advisory boards	65	36.3
Statutory bodies - Universities	7	3.9
Statutory TAFE institutes	2	1.1
Water boards	2	1.1
Other	2	1.1
<b>Total government agencies on frame</b>	<b>179</b>	<b>100.0*</b>

Note: \*Percentages may not add to exactly 100.0 due to rounding.

#### 3.3 Data collection method

The CCTV Survey 2011-12 was administered as an internet survey. Details on how to access and complete the web-based survey, including an individual login ID and password, were emailed to all government agency contacts on the survey frame. Government agencies invited to participate in the CCTV Survey 2011-12 could access the web-based questionnaire from Tuesday 15 November 2011, and could complete the questionnaire up until Monday 30 January 2012.

Reminder emails were sent to non-responding agencies on three separate occasions. These emails were used to improve response rates. The first reminder was sent on 29 November 2011, the second reminder on 6 December 2011, and the third and final reminder on 6 January 2012.

A Word document version of the questionnaire was also emailed to non-responding agencies on 22 November 2011. This was provided for their convenience in response to a number of requests, with instructions to distribute and complete the Word version survey as the agency saw fit. Once completed, responses were to be entered directly into the web version of the survey by each individual agency.

### 3.4 Final status and scope of agencies on frame

The final response status of government agencies on the Survey frame is described in Table 2. Almost 70% (68.2%) of agencies on the frame completed the CCTV questionnaire.

**Table 2** Final status of government agencies on frame

Final status	Frequency	Percentage (%)
Completed	122	68.2
Undeliverable	1	0.6
Unable/away	3	1.7
No response	50	27.9
Out of scope – hosted	3	1.7
<b>Total</b>	<b>179</b>	<b>100.0*</b>

Note: \*Percentages may not add to exactly 100.0 due to rounding.

Agencies were classified as **in-scope responding** if the agency completed or partially completed the survey.

Agencies were defined as **in-scope non-responding** if they:

- were invited to participate in the survey and did not provide any response;
- were unable to complete the survey due to the contact officer being away during the survey period; or
- had an invalid email address.

The balance, defined as **out-of-scope**, were agencies that larger parent agencies included as part of their survey response.

Table 3 describes the final status of the 176 in-scope government agencies.

**Table 3** Final status of in-scope government agencies

Status	Frequency	Percentage (%)
In-scope responding	122	69.3
In-scope non-responding	54	30.7
<b>Total in-scope agencies</b>	<b>176</b>	<b>100.0*</b>

Note: \*Percentages may not add to exactly 100.0 due to rounding.

### 3.5 Survey response rate

A measure of the quality of response achieved in a survey is the response rate. This is defined as the number of completed surveys as a percentage of the potential total number of surveys had every in-scope agency completed the survey. The CCTV Survey 2011-12 achieved a response rate of 69.3%.

Response rate = In-scope responding / Total in-scope  
= 122 / 176  
= 69.3%

A response rate of 69.3% is high for a web survey. A high response rate is more likely to minimise non-response bias and thus produce results that are representative of the population.

Table 4 describes the number of responding government agencies and response rates by respective agency type. The final sample of in-scope agencies is comprised of 46 local government councils, 46 statutory authorities and advisory boards, 12 government departments, six Queensland Health agencies, and 12 other government agencies.

**Table 4 Response rate by agency type**

	In-scope responding	In-scope non-responding	Total in-scope	Response rate (%)
Departments	12	1	13	92.3
Local government councils	46	28	74	62.2
Medical research institutes	1	0	1	100.0
Queensland Health agencies	6	7	13	46.2
Statutory authorities and advisory boards	46	16	62	74.2
Statutory bodies - Universities	5	2	7	71.4
Statutory TAFE institutes	2	0	2	100.0
Water boards	2	0	2	100.0
Other	2	0	2	100.0
<b>All agencies</b>	<b>122</b>	<b>54</b>	<b>176</b>	<b>69.3</b>

Note: Agencies defined as out-of-scope are excluded from response rate calculations.

A list of the in-scope non-responding agencies is included in Appendix 2.

Of the 13 government departments on the frame, the one in-scope non-responding department was the Department of Employment, Economic Development and Innovation (DEEDI). The survey was sent to an officer on long service leave whose emails were not being monitored. Upon the next DEEDI officer receiving the survey a five day time frame remained. Five days was insufficient time for an agency wide survey to be conducted and completed for such a diverse and regionalised agency. Accordingly, DEEDI regrettably advised it would not be providing a response to the survey, however, had obtained a copy of the survey to use as a guide in any possible future camera surveillance audits.

### 3.6 Respondent inquiries

A small number of enquiries were received in OESR's web mailbox and on the 1800 number. The majority of the enquiries were from respondents:

- advising that they had spoken directly to OIC regarding whether they had to complete the survey or not;
- notifying a change of email address, contact person, or details;
- providing feedback about their inability to complete the survey due to being on leave or overseas;
- requesting the email invitation be re-sent;
- calling with a query about the survey; or
- asking for an extension.

### 3.7 Data cleaning

Upon completion of the survey, consistency checks, data cleaning and editing were carried out. OESR checked the dataset to ensure that all skips and sequencing instructions had been applied correctly in the web system. The dataset was also checked to ensure there were no erroneous skips that had resulted in missing data. The main issues are below, together with the actions taken.

Responses that were recorded in the 'other specify' categories were checked and validated to ensure that they did not match an existing category. If they did, the response was recoded into this category. If a sufficiently large number of responses could be recoded into a category that was not a response option, a new category was created.

One government department was unable to answer Q1.2a-f because they felt that they could not adequately break down the purposes of all of their surveillance cameras using the available categories. The department indicated that their cameras were mainly used in service centres (retail stores and detention centres), but were unable to provide the total number that monitored within government buildings versus the precinct or immediate surroundings of government buildings. No cameras were used to monitor pedestrian or vehicle traffic. For the sake of simplicity, OESR (in consultation with OIC) attributed 50% of the department's cameras to monitoring within government buildings, 25% to monitoring the precinct or immediate surroundings of government buildings, and 25% to monitoring other areas (retail stores).

## 4 SURVEY RESULTS

### 4.1 Presentation and interpretation

This report summarises survey responses to the CCTV Survey 2011-12 at the whole of sample level, as well as results broken down by agency attributes where relevant. Results and comparisons are presented as a combination of text and/or tables, depending on the most appropriate method for displaying the data. Note that percentages presented in tables may not add up to exactly 100% due to rounding.

Due to the low sample size, statistical tests were not performed to determine whether apparent differences between groups were statistically significant. In general, if groups differed by less than 10% they were considered 'similar' and any differences in responses were assumed to be due to random variation and not of interest. Where comparisons between groups resulted in very small cell counts, comparisons were not undertaken at all.

The following points need to be kept in mind when interpreting the results presented in the report:

1. The agencies that responded to the survey represent a (not necessarily random) subset of all Queensland government agencies. For example, agencies that were less compliant with the IP Act may have been less inclined to respond to the survey. Therefore, the results reported here may not generalise to all agencies. As responses were not weighted to provide estimates for the entire population, some caution should be used when interpreting results.
2. The survey was conducted from November 2011 to January 2012 and provides a snapshot of selected agencies at that time. To reflect this, results are described in past tense and with reference to responding agencies.
3. The survey relied on self-reported information, which may not necessarily be an accurate portrayal of actual facts, figures and behaviours.
4. Sample size and cell counts were low for some of the questions and group comparisons. Response patterns may be unstable and should be interpreted with caution, as small changes in frequencies of response can have a large effect on percentages.

### 4.2 Comparison groups

A number of comparison groups were created based on the attributes of responding government agencies. Where sample size permitted, responses to each survey question were compared across groups and any differences noted in text.

Based on frame information government agencies were classified into three agency types:

- Government departments;
- Local government councils; and
- Public authorities (i.e. any remaining agencies).

A diverse range of government agencies were classified as public authorities. As such, the combined frequencies and percentages reported for this group may not accurately reflect their diversity of responses. Caution should therefore be taken when interpreting this information.

Based on responses to Q1.2g government agencies were also grouped by the total number of cameras they operated:

- 1 – 10 cameras;
- 11 – 100 cameras; and
- More than 100 cameras.

Based on responses to Q2.1a-h government agencies were divided by the degree to which they implemented documented policies and/or procedures for their camera surveillance systems, resulting in agencies with:

- Less than five documented policies and/or procedures; and
- Five or more documented policies and/or procedures.

As there were eight areas covered in Q2.1a-h for the purposes of this survey, agencies could adopt anywhere between zero and eight policies and/or procedures for their camera surveillance systems.

### 4.3 Surveillance camera deployment

All agencies were asked: *Does your agency operate surveillance cameras?* (Q1.1).

Of the 122 Queensland government agencies that responded to the survey, more than three in five (62.3%) operated surveillance cameras (Table 5). Government departments (75.0%) and local government councils (76.1%) appeared to be more likely than public authorities (50.0%) to operate surveillance cameras.

**Table 5 Whether government agencies operated surveillance cameras**

	Frequency	Percentage (%)
Operated surveillance cameras	76	62.3
Did not operate surveillance cameras	46	37.7
<b>Total</b>	<b>122</b>	<b>100.0</b>

Base: All agencies (n=122)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies that operated surveillance cameras were asked to provide the total number of cameras operated by their agency. (Q1.2g).

A total of 20,310 cameras were operated by the 76 government agencies that operated surveillance cameras. Government departments accounted for 67.1% of the total number of cameras operated by government agencies, with a further 17.8% of cameras operated by local government councils and 15.1% by public authorities (Table 6).

**Table 6 Total number of cameras operated, by agency type**

	Total	Percentage (%)	Agencies responding
Department	13,631	67.1	9
Local Government Council	3,609	17.8	35
Public Authority	3,070	15.1	32
<b>Total</b>	<b>20,310</b>	<b>100.0</b>	<b>76</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Of the agencies that operated surveillance cameras:

- Approximately one third (31.6%) operated between 1 and 10 cameras, one third (35.5%) operated between 11 and 100 cameras, and one third (32.9%) operated more than 100 cameras (Table 7).
- The majority (88.9%) of government departments operated more than 100 cameras, while local government councils (77.1%) and public authorities (71.9%) tended to operate 100 cameras or less.

**Table 7 Number of cameras operated by government agencies**

	Frequency	Percentage (%)
1 – 10 cameras	24	31.6
11 – 100 cameras	27	35.5
More than 100 cameras	25	32.9
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies that operated surveillance cameras were also asked to specify the number of cameras used for the purpose of monitoring different areas. (Q1.2a-f).

Over half (55.4%) of the cameras operated by government agencies were used for the purpose of monitoring within government buildings, with 15.8% for monitoring the precinct or immediate surroundings of government buildings, and 13.4% for monitoring pedestrian traffic (Table 8).

**Table 8 Monitoring purpose of cameras**

	Total	Percentage (%)
Within government buildings	11,243	55.4
Precinct or immediate surroundings of government buildings	3,215	15.8
Pedestrian traffic	2,719	13.4
Vehicle traffic	1,125	5.5
Public transport conveyances	310	1.5
Other areas	1,999	9.8
<b>Total number of cameras</b>	<b>20,310</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

The purpose of camera surveillance tended to differ between agency types. Government departments (80.5%) and public authorities (68.8%) used the majority of their surveillance cameras to monitor in and around government buildings, while local government councils split their use of camera surveillance evenly between monitoring pedestrian traffic (35.2%) and areas in and around government buildings (38.3%). Specifically:

- Government departments used almost two thirds of their cameras (63.4%) for monitoring within government buildings, with 17.1% used to monitor the precinct or immediate surroundings of government buildings. The remaining uses were for monitoring vehicle traffic (5.9%), pedestrian traffic (4.2%), public transport conveyances (0.4%), and other areas (9.1%).
- Public authorities used over half of their cameras (57.7%) for monitoring within government buildings, 28.8% for pedestrian traffic, and 11.1% for the precinct or

immediate surroundings of government buildings. The remaining uses were for monitoring vehicle traffic (1.0%) and other areas (8.1%).

- In contrast, local government councils used approximately one third (35.2%) of their cameras for monitoring pedestrian traffic, only 23.1% for monitoring within government buildings, and 15.2% for monitoring the precinct or immediate surroundings of government buildings. The remaining uses were for monitoring vehicle traffic (7.9%), public transport conveyances (7.0%), and other areas (14.2%).

Agencies that operated surveillance cameras were then asked: *Is footage of private property captured through your use of camera surveillance?* (Q1.3).

Of the 76 agencies that operated surveillance cameras, approximately one third (32.9%) captured footage of private property through their use of camera surveillance (Table 9).

**Table 9 Whether footage of private property captured through use of camera surveillance**

	Frequency	Percentage (%)
Captured footage of private property	25	32.9
Did not capture footage of private property	51	67.1
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), *Use of Camera Surveillance (CCTV) Survey 2011*.

Local government councils (45.7%) appeared to be the most likely to capture footage of private property, followed by government departments (33.3%) and public authorities (18.8%).

The number of cameras in operation may also be associated with capturing footage of private property. The greater the number of cameras operated by an agency, the greater the likelihood that footage of private property would be captured. Agencies that operated more than 100 cameras appeared to be the most likely (44.0%) to capture footage of private property, followed by agencies that operated 11 – 100 cameras (33.3%) and 1 – 10 cameras (20.8%).

#### 4.4 Policies and procedures to administer surveillance camera systems

Agencies that operated surveillance cameras were asked: *Does your agency have a documented policy and/or procedure for the following?* (Q2.1a-h).

Of the 76 agencies that operated surveillance cameras, over one quarter (26.3%) had no policies or procedures regarding their surveillance camera systems.

Over one half (53.9%) of agencies had five or more documented policies and/or procedures (Table 10).

**Table 10** Number of documented policies/procedures for surveillance camera systems

	Frequency	Percentage (%)
5 or more policies/procedures	41	53.9
Less than 5 policies/procedures	35	46.1
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

As shown in Table 12, over one half of agencies that operated surveillance cameras had a documented policy and/or procedure for the following:

- providing surveillance camera footage to others (59.2%);
- accessing surveillance camera footage (57.9%);
- instructions for staff operating the surveillance camera system (56.6%); and
- retention and disposal of surveillance camera footage (51.3%).

When comparing agency types, government departments (88.9%) appeared the most likely to have five or more policies/procedures in place, with local government councils (51.4%) and public authorities (46.9%) being of lower likelihood.

Implementation of policies and/or procedures for camera surveillance systems was also associated with the number of cameras operated by agencies.

- Agencies with over 100 cameras (80.0%) appeared to be more likely than agencies with 1 – 10 cameras (41.7%) or 11 – 100 cameras (40.7%) to have five or more documented policies/procedures in place.
- Furthermore, agencies that operated 11 – 100 cameras tended to be more likely than agencies with 1 – 10 cameras to indicate that policies and/or procedures for camera surveillance systems were in progress.

Agencies that operated surveillance cameras were asked: *Does your agency provide training to staff in surveillance camera system policies and procedures (beyond provision of operating manuals)?* (Q2.2).

Less than one third (31.6%) of government agencies provided training to staff in surveillance camera system policies and procedures (Table 11).

**Table 11** Whether training provided to staff in surveillance camera system policies and procedures

	Frequency	Percentage (%)
Training provided	24	31.6
Training not provided	31	40.8
In progress	13	17.1
Identified	8	10.5
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table 12 Status of documented policies/procedures for camera surveillance systems**

	Yes		No		In Progress		Identified		Total	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Instructions for staff operating the surveillance camera system	43	56.6	17	22.4	13	17.1	3	3.9	<b>76</b>	<b>100.0</b>
Managing surveillance camera records	34	44.7	15	19.7	22	28.9	5	6.6	<b>76</b>	<b>100.0</b>
Accessing surveillance camera footage	44	57.9	12	15.8	16	21.1	4	5.3	<b>76</b>	<b>100.0</b>
Retention and disposal of surveillance camera footage	39	51.3	14	18.4	13	17.1	10	13.2	<b>76</b>	<b>100.0</b>
Informing the community about the surveillance cameras	36	47.4	22	28.9	14	18.4	4	5.3	<b>76</b>	<b>100.0</b>
The use and limits of use of the surveillance camera footage	35	46.1	17	22.4	18	23.7	6	7.9	<b>76</b>	<b>100.0</b>
Providing surveillance camera footage to others	45	59.2	14	18.4	14	18.4	3	3.9	<b>76</b>	<b>100.0</b>
Evaluating the agency's surveillance system	28	36.8	27	35.5	16	21.1	5	6.6	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agency type, number of cameras, and policy implementation all appeared to be associated with providing training to staff in surveillance camera system policies and procedures. Specifically:

- Government departments (55.6%) appeared to be more likely than public authorities (37.5%) or local government councils (20.0%) to provide training to staff.
- Agencies that operated over 100 cameras (56.0%) also appeared to be more likely to provide training to staff than agencies that operated 1 – 10 cameras (25.0%) or 11 – 100 cameras (14.8%).
- Agencies with five or more policies/procedures for their camera surveillance systems (51.2%) appeared much more likely to provide their staff with training in surveillance camera system policies and procedures than agencies with less than five policies/procedures (8.6%).

#### 4.5 Purposes for implementation and use of surveillance camera systems

Agencies that operated surveillance cameras were asked: *What were the reasons for installing the camera surveillance system(s)?* (Q3.1a-k).

The most common reason for installing camera surveillance systems was property protection (89.5%), followed by crime prevention (77.6%), public safety (76.3%), crime investigation and enforcement (64.5%), and improving agency capacity to respond to issues (51.3%) (Table 13). The most common reasons for installing camera surveillance systems were similar across all agencies regardless of type, number of cameras, or policy implementation. See Tables A3a-c in Appendix 3 for more detailed information.

**Table 13 Reasons for installing camera surveillance systems**

	Frequency (out of 76 agencies)	Percentage (%)
Property protection	68	89.5
Crime prevention	59	77.6
Public safety	58	76.3
Crime investigation and enforcement	49	64.5
Improving agency capacity to respond to issues	39	51.3
Increase public perception of safety	30	39.5
Public demand or expectation	20	26.3
Staff safety	11	14.5
Traffic management	9	11.8
Research for a public interest	1	1.3
Other	8	10.5

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies that operated surveillance cameras were then asked: *What information or evidence supported the introduction of your camera surveillance system?* (Q3.3a-i).

The most common form of information or evidence that supported the introduction of camera surveillance systems was research into their effectiveness (40.8%) and evaluations of existing systems (36.8%) (Table 14).

Agency type, number of cameras, and policy implementation all appeared to be associated with the type of information and evidence used to support the introduction of camera surveillance systems. Specifically, government departments, agencies that operated more than 100 cameras, and agencies with five or more policies/procedures for their camera surveillance systems tended to cite more information and evidence to support the introduction of their camera surveillance systems than other agencies. See Tables A3d-f in Appendix 3 for more detailed information.

**Table 14** Information and evidence that supported introduction of camera surveillance systems

	Frequency (out of 76 agencies)	Percentage (%)
Research into the effectiveness of surveillance cameras	31	40.8
Evaluations of existing surveillance cameras	28	36.8
Privacy impact assessment	8	10.5
Identified need - vandalism/theft	8	10.5
Identified need - staff safety	7	9.2
Identified need - public concern	5	6.6
Other	19	25.0
None	5	6.6
Don't know	11	14.5

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Of the eight agencies that undertook a privacy impact assessment to support the introduction of camera surveillance systems, six also undertook research into the effectiveness of surveillance cameras, five undertook evaluations of existing surveillance cameras, two identified a need for staff safety, one identified a need to reduce or deter vandalism/theft, and two used other forms of information and evidence.

## 4.6 Notifying the community about camera surveillance

Agencies that operated surveillance cameras were asked: *Does your agency actively inform the community about the surveillance?* (Q4.1).

Over one half (56.6%) of government agencies that operated surveillance cameras actively informed the community about the surveillance (Table 15).

**Table 15 Whether community is actively informed about surveillance**

	Frequency	Percentage (%)
Actively informed community	43	56.6
Did not actively inform community	33	43.4
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Government departments (77.8%) were more likely than local government councils (60.0%) and public authorities (46.9%) to inform the community about their camera surveillance.

Agencies with more than 100 cameras (80.0%) were more likely than agencies with 1 – 10 cameras (45.8%) and 11 – 100 cameras (44.4%) to inform the community about their camera surveillance.

Agencies with five or more policies/procedures for their camera surveillance systems (61.0%) were somewhat more likely to inform the community about their camera surveillance than agencies with less than five policies/procedures (51.4%).

Agencies that actively informed the community about their camera surveillance were asked: *When notifying the community about the surveillance, how is the information provided?* (Q4.2a-e).

Over two thirds (67.4%) of agencies that operated surveillance cameras notified the community about the surveillance through a notice in the general area where cameras are used, 44.2% by a notice in the immediate vicinity of each camera, 34.9% on individual request, 30.2% in a publicly accessible document, and 16.3% through media releases (Table 16). See Table A3g in Appendix 3 for a summary of the overlap between how information is provided when notifying the community about camera surveillance.

**Table 16 How information is provided when notifying community about camera surveillance**

	Frequency (out of 43 agencies)	Percentage (%)
Notice in the general area where cameras are used	29	67.4
Notice in the immediate vicinity of each camera	19	44.2
On individual request	15	34.9
In a publicly accessible document	13	30.2
Media releases	7	16.3
Other	5	11.6

Base: Agencies that actively informed community about surveillance (n=43)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies with five or more policies/procedures and agencies with less than five policies/procedures for their camera surveillance systems informed the community about their camera surveillance in similar ways.

Due to low sample sizes and cell counts for this question, comparisons between agencies of different type and number of cameras were not carried out.

Agencies that actively informed the community about their camera surveillance were then asked: *Does the information provided to the community include the following?* (Q4.3a-i).

Approximately three in five (62.8%) agencies provided general information to the community about the purpose of the surveillance system. A further 27.9% provided information about whether it is the agency's usual practice to disclose footage to any other individual, agency, or organisation, and 20.9% on how to get access to the footage (Table 17).

**Table 17** Types of information provided to community about camera surveillance

	Frequency (out of 43 agencies)	Percentage (%)
Purpose of the surveillance system generally	27	62.8
Whether it is usual practice to disclose footage to any other individual, agency, or organisation	12	27.9
How to get access to the footage	9	20.9
Whether the surveillance is authorised or required under a law	6	14.0
If the surveillance is authorised or required under a law, information about the law	3	7.0
Purpose of the surveillance at each specific camera	2	4.7
If it is the agency's usual practice to disclose footage to any other individual, agency, or organisation, whether that individual, agency, or organisation would usually pass on the footage to another individual, agency, or organisation	2	4.7
Formats in which access to the footage can be obtained	1	2.3
None of the above	15	34.9

Base: Agencies that actively informed community about surveillance (n=43)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), *Use of Camera Surveillance (CCTV) Survey 2011*.

Due to low sample sizes and cell counts for this question, comparisons between agencies of different type, number of cameras, and policy implementations were not carried out.

## 4.7 Data storage and security of camera surveillance footage

Agencies that operated surveillance cameras were asked:

*Where is your surveillance camera footage stored?* (Q5.1a-f).

*Access to surveillance camera footage is managed by the following?* (Q5.2a-i).

The majority of agencies (88.2%), irrespective of type, number of cameras, or policy implementation, stored their surveillance camera footage in their own agency facilities (Table 18).

Local government councils (11.4%) and public authorities (9.4%) may be somewhat more likely than government departments (0.0%) to store their camera footage in another government agency's facilities. Local government councils (14.3%) may also be somewhat more likely than public authorities (3.1%) and government departments (0.0%) to store their footage in a private sector contractor's facilities.

**Table 18 Where surveillance camera footage is stored**

	Frequency (out of 76 agencies)	Percentage (%)
Agency facilities	67	88.2
Another government agency's facilities	7	9.2
Private sector contractor's facilities	6	7.9
Other	5	6.6
Footage is not stored anywhere	1	1.3
Don't know	1	1.3

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Almost all (96.1%) government agencies that operated surveillance cameras managed access to their camera footage.

The majority (88.2%) of agencies only allow individuals to access the footage if authorised to do so, 68.4% store the footage under password protection, 64.5% subject the footage to physical security measures, 43.4% document access to the footage, 38.2% have documented security procedures to govern access by external individuals, agencies, or organisations, and 11.8% subject the footage to data encryption (Table 19).

**Table 19 How access to surveillance camera footage is managed**

	Frequency (out of 76 agencies)	Percentage (%)
Individuals can only access the footage if authorised to do so	67	88.2
Footage is stored under password protection	52	68.4
Footage is subject to physical security measures	49	64.5
Access to the footage is documented	33	43.4
Access by external individuals, agencies, and organisations is governed by documented security procedures	29	38.2
Footage is subject to data encryption	9	11.8
Other	4	5.3
Footage is not managed formally	3	3.9

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Government departments appeared to implement a greater number of formal management procedures for their surveillance camera footage than either local government councils or public authorities.

Agencies that operated 1 – 10 surveillance cameras appeared to implement fewer formal management procedures than agencies that operated 11 – 100 cameras or over 100 cameras.

Agencies with five or more policies/procedures for their camera surveillance systems appeared to implement a somewhat greater number of formal management procedures than agencies with less than five policies/procedures.

See Tables A3h-j in Appendix 3 for more detailed information.

## 4.8 Disclosure of camera surveillance footage

Agencies that operated surveillance cameras were asked: *Does your agency have an administrative arrangement with any of the following entities concerning access to camera surveillance footage?* (Q6.1a-d).

Over one half (52.6%) of government agencies had an administrative arrangement with another agency concerning access to their camera surveillance footage: 42.1% had an administrative arrangement with the Queensland Police Service, 11.8% with another government agency (excluding the Queensland Police Service), and 6.6% with a non-government organisation (Table 20).

**Table 20** Type of organisations with administrative arrangements concerning access to camera surveillance footage

	Frequency (out of 76 agencies)	Percentage (%)
Queensland Police Service	32	42.1
Other government agencies	9	11.8
Other organisations	5	6.6
None of the above	36	47.4

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Government departments (77.8%) appeared to have a higher incidence of administrative arrangements with the Queensland Police Service concerning access to their camera surveillance footage than local government councils (54.3%) and public authorities (18.8%). Public authorities (15.6%) and local government councils (11.4%) appeared to be more likely than government departments (0.0%) to have administrative arrangements with another government agency.

Agencies that operated more than 100 cameras (72.0%) were more likely than agencies with 11 – 100 cameras (44.4%) or 1 – 10 cameras (8.3%) to have an administrative arrangement with the Queensland Police Service.

Agencies with five or more policies/procedures for their camera surveillance systems appeared more to have a higher incidence of administrative arrangements with the Queensland Police Service (56.1%) and other government agencies (19.5%), than agencies with less than five policies/procedures (25.7% and 2.9% respectively).

Agencies that had an administrative arrangement with another organisation concerning access to camera surveillance footage were asked: *Does this access occur according to a formal written agreement or in accordance with an established procedure?* (Q6.2).

Of the 40 agencies that had an administrative arrangement with another organisation, the majority (80.0%) allowed access to their camera surveillance footage according to a formal written agreement or in accordance with an established procedure (Table 21).

**Table 21 Whether access to footage by other organisations occurs according to a formal written agreement or established procedure**

	Frequency	Percentage (%)
Formal agreement or established procedure	32	80.0
No formal agreement or established procedure	8	20.0
<b>Total</b>	<b>40</b>	<b>100.0</b>

Base: Agencies with an administrative arrangement with other organisations concerning access to surveillance footage (n=40)  
Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Local government councils (90.9%) appeared to be more likely than government departments (71.4%) and public authorities (63.6%) to have a formal written agreement or established procedure in place.

Agencies that operated 11 – 100 cameras (86.7%) or more than 100 cameras (80.0%) also appeared more likely than agencies with 1 – 10 cameras (60.0%) to have a formal written agreement or established procedure in place.

## 4.9 Private contractors for surveillance camera systems

Agencies that operated surveillance cameras were asked: *Is your agency's camera surveillance system operated in part or fully by a private sector contractor?* (Q7.1).

Over one quarter (27.6%) of agencies that operated camera surveillance systems indicated that their surveillance systems were operated in part or fully by a private sector contractor (Table 22).

**Table 22 Whether camera surveillance systems operated in part or fully by private sector contractors**

	Frequency	Percentage (%)
Operated in part or fully by private sector contractor	21	27.6
Not operated in part or fully by private sector contractor	55	72.4
<b>Total</b>	<b>76</b>	<b>100.0</b>

Base: Agencies that operated surveillance cameras (n=76)  
Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Local government councils (42.9%) and government departments (33.3%) appeared more likely than public authorities (9.4%) to have a private sector contractor operate their camera surveillance systems.

Agencies that operated more than 100 cameras (56.0%) appeared to be more likely than agencies that operated 11 – 100 cameras (18.5%) or 1 – 10 cameras (8.3%) to have a private sector contractor operate their camera surveillance systems.

Agencies with five or more policies/procedures for their camera surveillance systems (34.1%) appeared to be somewhat more likely to have a private sector contractor operate their camera surveillance systems than agencies with less than five policies/procedures (20.0%).

Agencies whose camera surveillance system was operated in part or fully by a private sector contractor were asked:

*When was the contract for operating the surveillance camera system entered into? (Q7.2).  
If there is a contract, does it cover the following items? (Q7.4a-f).*

Of the 21 agencies whose camera surveillance system was operated in part or fully by a private sector contractor, 61.9% entered into a contract before 30 June 2009 (Table 23).

**Table 23 Date that contracts with private sector contractors were entered into**

	Frequency	Percentage (%)
Before 30 June 2009	13	61.9
Between 1 July 2009 - 30 June 2010	2	9.5
Between 1 July 2010 - 30 June 2011	6	28.6
<b>Total</b>	<b>21</b>	<b>100.0</b>

Base: Agencies whose camera surveillance was operated by private sector contractor (n=21)

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Two thirds (66.7%) of the agencies whose camera surveillance system was operated in part or fully by a private sector contractor had contracts which covered access to the footage, and the safety and security of the footage. Approximately 60% (61.9%) had contracts which covered the disclosure of footage to third parties, and over one half (52.4%) had contracts which covered the secondary use of footage, and the retention and disposal of footage (Table 24).

**Table 24 Items covered in contracts with private sector contractors**

	Frequency (out of 21 agencies)	Percentage (%)
Safety and security of footage	14	66.7
Access to footage	14	66.7
Disclosure of footage to third parties	13	61.9
Secondary use of footage	11	52.4
Retention and disposal of footage	11	52.4
None of the above	6	28.6

Base: Agencies whose camera surveillance was operated by private sector contractor (n=21)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies with five or more policies/procedures for their camera surveillance systems appeared to be more likely than agencies with less than five policies/procedures to cover the aforementioned items in their contracts with private sector contractors.

Due to low sample sizes and cell counts for this question, comparisons between agencies of different type and number of cameras were not carried out.

Local government agencies whose contract was entered into on or after 1 July 2010 and any other government agencies whose contract was entered into on or after 1 July 2009 were then asked: *Was the contractor bound by the contract to compliance with the privacy principles in the IP Act?* (Q7.3a/b).

As shown in Table 25, five out of six agencies (83.3%) had a contract which bound the contractor to compliance with the privacy principles in the IP Act. All six agencies entered into a contract with a private sector contractor between 1 July 2010 and 30 June 2011.

The agency that did not enter into a contract which bound the contractor to compliance with the privacy principles in the IP Act was a local government agency.

**Table 25 Whether contractors were bound to compliance with privacy principles in the IP Act**

	Frequency	Percentage (%)
Contractor bound to compliance	5	83.3
Contractor not bound to compliance	1	16.7
<b>Total</b>	<b>6</b>	<b>100.0</b>

Base: Local government agencies whose contract was entered into on or after 1 July 2010 and any other government agencies whose contract was entered into on or after 1 July 2009 (n=6)  
Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Due to low sample sizes and cell counts for this question, comparisons between agencies of different type, number of cameras, and policy implementations were not carried out.

#### 4.10 Passing camera surveillance footage outside Australia

Agencies that operated surveillance cameras were asked:

*Is the camera footage available on the internet?* (Q8.1a).

*Is the camera footage stored offshore, e.g. in the cloud, or with a contractor or service provider located outside Australia?* (Q8.1b).

*Is the camera footage passed outside Australia by any other means?* (Q8.1c).

The majority of agencies (94.7%) did not pass their camera footage outside of Australia: only 5.3% of agencies had the camera footage available on the internet, and 1.3% stored the camera footage offshore (Table 26).

**Table 26 Whether camera surveillance footage was passed outside Australia**

	Frequency (out of 76 agencies)	Percentage (%)
Camera footage available on the internet	4	5.3
Camera footage stored offshore	1	1.3
Camera footage passed outside Australia by other means	0	0.0

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may not add to sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

Agencies that passed their camera footage outside of Australia were asked: *Does your agency have a policy and/or procedure to ensure compliance with the privacy obligations surrounding transfer of personal information outside Australia (section 33 of the IP Act)?* (Q8.2).

Of the four agencies that passed their surveillance camera footage outside of Australia, two had a policy and/or procedure to ensure compliance with the privacy obligations surrounding transfer of personal information outside Australia.

Due to low sample sizes and cell counts for these questions, comparisons between agencies of different type, number of cameras, and policy implementations were not carried out.

## 5 GLOSSARY

This glossary provides information about statistical terminology used in the report.

Frame – a list, map, or conceptual specification of the people or other units comprising the survey population from which respondents can be selected. Examples include a telephone or city directory, or a list of members of a particular association or group.

Population – any entire group with at least one characteristic in common, for example, residents of Queensland.

Respondent – the person who is interviewed.

Response rate – the percentage of a sample from which information is successfully obtained. Response rates are calculated differently depending on the survey organisation.

Sample – part of a population. It is a subset of the population, often randomly selected for the purpose of studying the characteristics of the entire population.

Scope – is the term used to describe people or other entities that could potentially be part of a particular survey. For the Use of Camera Surveillance Survey 2011-12, public authorities which are defined in the Right to Information legislation as being established for a public purpose by, or under, an Act are in-scope; all other entities, including those where larger parent agencies included them as part of their survey response, are out-of-scope.

## 6 APPENDICES

### Appendix 1 – Survey instrument

#### Office of the Information Commissioner Information Privacy and Camera Surveillance Use By Qld Govt Agencies Survey 2011

##### Background Information

The *Information Privacy Act 2009* (IP Act) provides safeguards for the handling of personal information in the public sector environment, and allows access to and amendment of personal information.

Under Section 135 of the IP Act, the Information Commissioner can conduct reviews into personal information handling practices of agencies and conduct compliance audits to assess agency compliance with the privacy principles.

Queensland State Archive's *Guideline for Managing Closed Circuit Television Records* provides further information about the management of surveillance footage as public records, in accordance with the requirements of the *Information Privacy Act 2009*.

##### Purpose of this Survey

This survey will assist the Office of the Information Commissioner to fulfil its legislative requirements to monitor and report on the extent to which agencies are complying with the IP Act in their implementation and use of camera surveillance systems.

The survey results will identify the purposes for which camera surveillance systems have been installed and provide an indication of how well the general administration of the system complies with the privacy principles.

The Office of the Information Commissioner will report on its findings and provide recommendations as necessary to improve agency compliance with the privacy obligations in the IP Act. Agency survey results will be represented in the report in aggregate form only, either within the total respondent agencies or relevant sector (eg. local government agencies). The final report will be presented to the Speaker for tabling in the Legislative Assembly.

All data collected is strictly confidential and will be de-identified before publication.

#### INSTRUCTIONS ON HOW TO COMPLETE THIS SURVEY

1. Please complete the survey by selecting the appropriate box next to the relevant answers.
2. If the relevant information is to hand, the survey takes about 10 minutes to complete. Information concerning camera surveillance hardware can be accessed through agency asset registers.
3. There is a comment box at the end of the survey, in which comments can be made to identify additional responses that were not catered for in the set options, and for general comments. Please make as many comments as desired.
4. For any enquiries regarding the content of the survey, please contact Karen McLeod on (07) 3405 3068 or email [Karen.McLeod@oic.qld.gov.au](mailto:Karen.McLeod@oic.qld.gov.au).
5. For enquiries regarding the online lodgement of the survey, please contact the Office of the Government Statistician on 1800 068 587, or email [oesr.websurvey@treasury.qld.gov.au](mailto:oesr.websurvey@treasury.qld.gov.au).

#### INSTRUCTIONS ON HOW TO SAVE AND SUBMIT THE SURVEY

The **SAVE** button that has been provided at the bottom of each page can be used if you cannot or do not want to complete the survey in one sitting. Press the **SAVE** button at any time and the information you have already provided will be saved and you can return to complete your survey.

*(Please Note: DO NOT use the Internet Browser Save button at the top left hand side of the page under File to save your responses).*

Your unique login and password will allow you to access your partially completed survey.

When you have finished the survey, please click on the **SUBMIT** button.

For security purposes, once your survey has been submitted it will no longer be accessible online.

Thank you for completing the Information Privacy and Camera Surveillance Use by Queensland Government Agencies Survey.

#### DEFINITIONS

**"Surveillance camera" –**

means the use of video cameras to transmit a signal to a specific place, to a storage medium and/or a limited set of monitors. 'Surveillance camera' includes but is not restricted to 'closed circuit television' (CCTV). 'Surveillance camera' does not include non-fixed or mobile camera systems such as speed cameras. Nor does 'surveillance camera' include covert surveillance systems.

The survey covers "public spaces" which are itemised in Question 1.2.

## SURVEILLANCE CAMERA DEPLOYMENT

\* 1.1. Does your agency operate surveillance cameras?

☐ Yes

☐ No – Go to Q10

\* 1.2. How many cameras are used for the purpose of monitoring:

*Please place a number in the box for each option that applies. If an option does not apply, please type '0'.*

*(NOTE: All purposes for each camera should be selected where there are multiple purposes. The total number of cameras is recorded separately at the end of this section.)*

Pedestrian traffic (eg. - malls, parks, public car parks, transport hubs) \_\_\_\_\_

Vehicle traffic (eg. - on highways, roads, railway lines) \_\_\_\_\_

Public transport conveyances (eg. - inside buses, train coaches, ferries) \_\_\_\_\_

Within government buildings \_\_\_\_\_

The precinct or immediate surroundings of a government building (eg. - grounds, yards, depots) \_\_\_\_\_

Other areas \_\_\_\_\_ (Please specify other areas in Q1.2h)

TOTAL NUMBER OF CAMERAS OPERATED BY AGENCY \_\_\_\_\_

\* 1.2h. Please specify the other areas in which cameras are used for the purpose of monitoring.

---

---

---

\* 1.3. Is footage of private property captured through your use of camera surveillance?

☐ Yes

☐ No

## POLICIES AND PROCEDURES TO ADMINISTER SURVEILLANCE CAMERA SYSTEMS

\* 2.1. Does your agency have a documented policy and/or procedure for the following?

(Please answer for each option)

**PLEASE NOTE:**

*In progress* - This means that management has decided on a particular course of action, and implementation has commenced or is complete in part but not all of the agency.

*Identified* - This means that management has identified this as an issue, but has not yet commenced to address the issue.

	Yes	No	In progress	Identified
Instructions for staff operating the surveillance camera system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Managing surveillance camera records (including footage and other records)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Accessing surveillance camera footage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Retention and disposal of surveillance camera footage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Informing the community about the surveillance cameras	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use and limits of use of the surveillance camera footage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Providing surveillance camera footage to others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Evaluating the agency's surveillance system, particularly with respect to the purpose for installing the system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

\* 2.2. Does your agency provide training to staff in surveillance camera system policies and procedures (beyond provision of operating manuals)?

**PLEASE NOTE:**

*In progress* - This means that management has decided on a particular course of action, and implementation has commenced or is complete in part but not all of the agency.

*Identified* - This means that management has identified this as an issue, but has not yet commenced to address the issue.

- ☐ Yes
- ☐ No
- ☐ In progress
- ☐ Identified

## PURPOSES FOR IMPLEMENTATION AND USE OF SURVEILLANCE CAMERA SYSTEMS

\* 3.1. What were the reasons for installing the camera surveillance system(s)?

*(Please select each reason that applies)*

- ☐ Public safety
- ☐ Property protection
- ☐ Crime prevention
- ☐ Crime investigation and enforcement
- ☐ Research for a public interest *(please specify)* \_\_\_\_\_
- ☐ Increase public perception of safety
- ☐ Public demand or expectation
- ☐ Traffic management
- ☐ Improving agency capacity to respond to issues (eg. observing incidents that might need expedient agency intervention)
- ☐ Other *(please specify)* \_\_\_\_\_

\* 3.2a. Does your agency use the surveillance footage for any other reasons?

☐ Yes (please specify) \_\_\_\_\_

☐ No

\* 3.3. What information or evidence supported the introduction of your camera surveillance system?

*(Please select each option that applies)*

☐ Research into the effectiveness of surveillance cameras

☐ Privacy impact assessment

☐ Evaluations of existing surveillance cameras

☐ Other (please specify) \_\_\_\_\_

☐ None

☐ Don't know

## NOTIFYING THE COMMUNITY ABOUT THE SURVEILLANCE

\* 4.1. Does your agency actively inform the community about the surveillance?

- ☐ Yes
- ☐ No Go to Q5:

\* 4.2. When notifying the community about the surveillance, how is the information provided?

*(Please select each option that applies)*

- ☐ By a notice in the immediate vicinity of each camera
- ☐ By a notice in the general area where cameras are used (eg. at the entrances to pedestrian malls or buildings)
- ☐ In a publicly accessible document (eg. on the agency's website)
- ☐ On individual request
- ☐ Other *(please specify)* \_\_\_\_\_

\* 4.3. Does the information provided to the community include the following?

*(Please select each option that applies)*

- ☐ The purpose of the surveillance system generally
- ☐ The purpose of the surveillance at each specific camera
- ☐ Whether the surveillance is authorised or required under a law
- ☐ If the surveillance is authorised or required under a law, information about the law
- ☐ Whether it is the agency's usual practice to disclose footage to any other individual, agency, or organisation
- ☐ If it is the agency's usual practice to disclose footage to any other individual, agency, or organisation, whether that individual, agency, or organisation would usually pass on the footage to another individual, agency, or organisation
- ☐ How to get access to the footage
- ☐ The formats in which access to the footage can be obtained
- ☐ None of the above

## DATA STORAGE AND SECURITY

\* 5.1. Where is your surveillance camera footage stored?

*(Please select each option that applies)*

- ☐ Agency facilities
- ☐ Another government agency's facilities
- ☐ Private sector contractor's facilities
- ☐ Other *(please specify)* \_\_\_\_\_
- ☐ Footage is not stored anywhere
- ☐ Don't know

\* 5.2. Access to surveillance camera footage is managed by the following:

*(Please select each option that applies)*

- ☐ Individuals can only access the footage if authorised to do so
- ☐ Footage is subject to data encryption
- ☐ Footage is stored under password protection
- ☐ Access to the footage is documented, eg. in a log, to create an audit trail
- ☐ Access by external individuals, agencies, and organisations is governed by documented security procedures
- ☐ Footage is subject to physical security measures, eg. locked storage
- ☐ Other *(please specify)* \_\_\_\_\_
- ☐ Footage is not managed formally
- ☐ Don't know

## DISCLOSURE OF THE CAMERA SURVEILLANCE FOOTAGE

\* **6.1.** Does your agency have an administrative arrangement with any of the following entities concerning access to camera surveillance footage?

*(Please select each option that applies)*

☐ Other government agencies, eg. to the Queensland Police Service for law enforcement purposes  
*(please specify)* \_\_\_\_\_

☐ Other organisations *(please specify)* \_\_\_\_\_

☐ None of the above GO TO Q7

\* **6.2a.** Does this access occur according to a formal written agreement or in accordance with an established procedure?

☐ Yes *(please specify)* \_\_\_\_\_

☐ No

## CONTRACTORS

\* **7.1a.** Is your agency's camera surveillance system operated in part or fully by a private sector contractor?

- ☐ Yes (*please specify*) \_\_\_\_\_
- ☐ No Go to Q8:

\* **7.2.** When was the contract for operating the surveillance camera system entered into?

- ☐ Before 30 June 2009: Go to Q7.4:
- ☐ Between 1 July 2009 - 30 June 2010
- ☐ Between 1 July 2010 - 30 June 2011
- ☐ Between 1 July 2011 - 30 June 2012

If you are a non-local government agency and the contract was entered into after 1 July 2009:

\* **7.3a.** If the contract was entered into after 1 July 2009, was the contractor bound by the contract to compliance with the privacy principles in the IP Act?

- ☐ Yes
- ☐ No

If you are a local government agency and the contract was entered into after 1 July 2010:

\* **7.3b.** If the contract was entered into after 1 July 2010, was the contractor bound by the contract to compliance with the privacy principles in the IP Act?

- ☐ Yes
- ☐ No

\* 7.4. If there is a contract, does it cover the following items?

*(Please select each option that applies)*

- ☐ Safety and security of footage
- ☐ Access to footage
- ☐ Secondary use of footage, ie. use of the footage for a purpose other than that for which the camera was initially installed and operated
- ☐ Disclosure of footage to third parties
- ☐ Retention and disposal of footage
- ☐ None of the above

## OUTSIDE AUSTRALIA

This section is about whether the footage passes outside Australia.

\* **8.1a.** Is the camera footage available on the internet?

☐ Yes

☐ No

\* **8.1b.** Is the camera footage stored offshore, eg. in the cloud, or with a contractor or service provider located outside Australia?

☐ Yes

☐ No

\* **8.1c.** Is the camera footage passed outside Australia by any other means?

☐ Yes (please specify) \_\_\_\_\_

☐ No

If 8.1a, 8.1b, or 8.1c = Yes, then go to 8.2.

Otherwise skip to 9.

\* **8.2.** Does your agency have a policy and/or procedure to ensure compliance with the privacy obligations surrounding transfer of personal information outside Australia (section 33 of the IP Act)?

**PLEASE NOTE:**

*In progress* - This means that management has decided on a particular course of action, and implementation has commenced or is complete in part but not all of the agency.

*Identified* - This means that management has identified this as an issue, but has not yet commenced to address the issue.

☐ Yes

☐ No

☐ In progress

☐ Identified

9. Are there any other comments that you wish to make regarding camera surveillance usage by your agency?

---

---

---

10. Are there any comments that you would like to make about this survey?

---

---

---

Thank you for completing the survey.

For security purposes, once your Information Privacy and Camera Surveillance Use By Qld Govt Agencies Survey 2011 has been submitted, it will no longer be accessible online.

## **Appendix 2 – List of non-responding agencies**

### **Government Departments**

Department of Employment, Economic Development & Innovation

### **Local Government Councils**

Blackall-Tambo Regional Council  
Boulia Shire Council  
Bundaberg Regional Council  
Burke Shire Council  
Cairns Regional Council  
Carpentaria Shire Council  
Cloncurry Shire Council  
Doomadgee Aboriginal Shire Council  
Goondiwindi Regional Council  
Hope Vale Aboriginal Shire Council  
Kowanyama Aboriginal Shire Council  
Lockhart River Aboriginal Shire Council  
Longreach Regional Council  
Mackay Regional Council  
Mapoon Aboriginal Shire Council  
Mornington Shire Council  
Mt Isa City Council  
Napranum Aboriginal Shire Council  
Palm Island Aboriginal Shire Council  
Pompuraaw Aboriginal Shire Council  
Redland City Council  
Richmond Shire Council  
South Burnett Regional Council  
Torres Shire Council  
Torres Strait Island Regional Council  
Weipa Town Council  
Whitsunday Regional Council  
Winton Shire Council

### **Public Authorities**

Aboriginal Centre for the Performing Arts  
Brisbane Festival  
Disability Council of Queensland Secretariat  
Gladstone Economic and Industry Development Board  
Griffith University  
Health Quality and Complaints Commission  
James Cook University  
National Trust of Queensland  
Princess Alexandra Foundation  
Prince Charles Hospital Foundation  
Queensland Audit Office  
Queensland Bulk Water Supply Authority trading as SEQWater  
Queensland Health Community Councils  
Queensland Rural Adjustment Authority  
Queensland Water Commission  
Queensland Workplace Rights Ombudsman  
Redcliffe Hospital Foundation  
South-East Queensland Water Grid Manager

Southern Regional Water Pipeline Company Pty Ltd trading as LinkWater Projects  
Sunshine Coast Health Foundation  
Supreme Court of Queensland Library  
Toowoomba Hospital Foundation  
Townsville Entertainment and Convention Centre  
Townsville Hospital Foundation  
Wet Tropics Management Authority (Board of Directors)



## Appendix 3 – Output tables

**Table A3a Reasons for installing camera surveillance systems, by agency type**

	Department		Local Government Council		Public Authority	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Property protection	9	100.00	31	88.6	28	87.5
Crime prevention	9	100.00	28	80.0	22	68.8
Public safety	9	100.00	26	74.3	23	71.9
Crime investigation and enforcement	8	88.9	28	80.0	13	40.6
Improving agency capacity to respond to issues	6	66.7	13	37.1	20	62.5
Increase public perception of safety	4	44.4	17	48.6	9	28.1
Public demand or expectation	3	33.3	13	37.1	4	12.5
Staff safety	2	22.2	1	2.9	8	25.0
Traffic management	2	22.2	4	11.4	3	9.4
Research for a public interest	0	0.0	1	2.9	0	0.0
Other	4	44.4	3	8.6	1	3.1
<b>Number of agencies</b>	<b>9</b>		<b>35</b>		<b>32</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3b Reasons for installing camera surveillance systems, by number of cameras**

	1 – 10 cameras		11 – 100 cameras		More than 100 cameras	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Property protection	19	79.2	25	92.6	24	96.0
Crime prevention	14	58.3	22	81.5	23	92.0
Public safety	14	58.3	19	70.4	25	100.0
Crime investigation and enforcement	12	50.0	15	55.6	22	88.0
Improving agency capacity to respond to issues	8	33.3	11	40.7	20	80.0
Increase public perception of safety	7	29.2	10	37.0	13	52.0
Public demand or expectation	3	12.5	8	29.6	9	36.0
Staff safety	5	20.8	3	11.1	3	12.0
Traffic management	2	8.3	0	0.0	7	28.0
Research for a public interest	0	0.0	1	3.7	0	0.0
Other	2	8.3	2	7.4	4	16.0
<b>Number of agencies</b>	<b>24</b>		<b>27</b>		<b>25</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed.

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3c Reasons for installing camera surveillance systems, by policy implementation**

	5 or more policies/procedures		Less than 5 policies/procedures	
	Frequency	Percentage (%)	Frequency	Percentage (%)
Property protection	38	92.7	30	85.7
Crime prevention	33	80.5	26	74.3
Public safety	37	90.2	21	60.0
Crime investigation and enforcement	31	75.6	18	51.4
Improving agency capacity to respond to issues	24	58.5	15	42.9
Increase public perception of safety	17	41.5	13	37.1
Public demand or expectation	12	29.3	8	22.9
Staff safety	6	14.6	5	14.3
Traffic management	6	14.6	3	8.6
Research for a public interest	0	0.0	1	2.9
Other	4	9.8	4	11.4
<b>Number of agencies</b>	<b>41</b>		<b>35</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3d Information and evidence that supported introduction of camera surveillance systems, by agency type**

	Department		Local Government Council		Public Authority	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Research into the effectiveness of surveillance cameras	7	77.8	15	42.9	9	28.1
Evaluations of existing surveillance cameras	8	88.9	11	31.4	9	28.1
Privacy impact assessment	1	11.1	4	11.4	3	9.4
Identified need - vandalism/theft	0	0.0	5	14.3	3	9.4
Identified need - staff safety	1	11.1	2	5.7	4	12.5
Identified need - public concern	1	11.1	4	11.4	0	0.0
Other	6	66.7	6	17.1	7	21.9
None	0	0.0	4	11.4	1	3.1
Don't know	0	0.0	4	11.4	7	21.9
<b>Number of agencies</b>	<b>9</b>		<b>35</b>		<b>32</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3e Information and evidence that supported introduction of camera surveillance systems, by number of cameras**

	1 – 10 cameras		11 – 100 cameras		More than 100 cameras	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Research into the effectiveness of surveillance cameras	6	25.0	11	40.7	14	56.0
Evaluations of existing surveillance cameras	4	16.7	9	33.3	15	60.0
Privacy impact assessment	2	8.3	2	7.4	4	16.0
Identified need - vandalism/theft	4	16.7	4	14.8	0	0.0
Identified need - staff safety	4	16.7	0	0.0	3	12.0
Identified need - public concern	2	8.3	0	0.0	3	12.0
Other	3	12.5	4	14.8	12	48.0
None	2	8.3	3	11.1	0	0.0
Don't know	5	20.8	4	14.8	2	8.0
<b>Number of agencies</b>	<b>24</b>		<b>27</b>		<b>25</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3f Information and evidence that supported introduction of camera surveillance systems, by policy implementation**

	5 or more policies/procedures		Less than 5 policies/procedures	
	Frequency	Percentage (%)	Frequency	Percentage (%)
Research into the effectiveness of surveillance cameras	20	48.8	11	31.4
Evaluations of existing surveillance cameras	21	51.2	7	20.0
Privacy impact assessment	5	12.2	3	8.6
Identified need - vandalism/theft	4	9.8	4	11.4
Identified need - staff safety	5	12.2	2	5.7
Identified need - public concern	5	12.2	0	0.0
Other	11	26.8	8	22.9
None	1	2.4	4	11.4
Don't know	3	7.3	8	22.9
<b>Number of agencies</b>	<b>41</b>		<b>35</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3g Overlap between how information is provided when notifying community about camera surveillance**

	Notice in the general area where cameras are used		Notice in the immediate vicinity of each camera		On individual request		In a publicly accessible document		Media releases		Other	
	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%	Frequency	%
Notice in the general area where cameras are used	-	-	11	57.9	12	80.0	9	69.2	4	57.1	3	60.0
Notice in the immediate vicinity of each camera	11	37.9	-	-	7	46.7	8	61.5	4	57.1	2	40.0
On individual request	12	41.4	7	36.8	-	-	6	46.2	3	42.9	3	60.0
In a publicly accessible document	9	31.0	8	42.1	6	40.0	-	-	5	71.4	3	60.0
Media releases	4	13.8	4	21.1	3	20.0	5	38.5	-	-	3	60.0
Other	3	10.3	2	10.5	3	20.0	3	23.1	3	42.9	-	-
<b>Number of agencies</b>	<b>29</b>		<b>19</b>		<b>15</b>		<b>13</b>		<b>7</b>		<b>5</b>	

Base: Agencies that actively informed community about surveillance (n=43)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3h How access to surveillance camera footage is managed, by agency type**

	Department		Local Government Council		Public Authority	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Individuals can only access the footage if authorised to do so	9	100.0	29	82.9	29	90.6
Footage is stored under password protection	7	77.8	22	62.9	23	71.9
Footage is subject to physical security measures	7	77.8	22	62.9	20	62.5
Access to the footage is documented	7	77.8	12	34.3	14	43.8
Access by external individuals, agencies, and organisations is governed by documented security procedures	6	66.7	13	37.1	10	31.3
Footage is subject to data encryption	2	22.2	5	14.3	2	6.3
Other	2	22.2	1	2.9	1	3.1
Footage is not managed formally	0	0.0	2	5.7	1	3.1
<b>Number of agencies</b>	<b>9</b>		<b>35</b>		<b>32</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3i** How access to surveillance camera footage is managed, by number of cameras

	1 – 10 cameras		11 – 100 cameras		More than 100 cameras	
	Frequency	Percentage (%)	Frequency	Percentage (%)	Frequency	Percentage (%)
Individuals can only access the footage if authorised to do so	18	75.0	26	96.3	23	92.0
Footage is stored under password protection	9	37.5	23	85.2	20	80.0
Footage is subject to physical security measures	12	50.0	18	66.7	19	76.0
Access to the footage is documented	5	20.8	10	37.0	18	72.0
Access by external individuals, agencies, and organisations is governed by documented security procedures	2	8.3	8	29.6	19	76.0
Footage is subject to data encryption	1	4.2	2	7.4	6	24.0
Other	0	0.0	0	0.0	4	16.0
Footage is not managed formally	3	12.5	0	0.0	0	0.0
<b>Number of agencies</b>	<b>24</b>		<b>27</b>		<b>25</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.



**Table A3j** How access to surveillance camera footage is managed, by policy implementation

	5 or more policies/procedures		Less than 5 policies/procedures	
	Frequency	Percentage (%)	Frequency	Percentage (%)
Individuals can only access the footage if authorised to do so	37	90.2	30	85.7
Footage is stored under password protection	28	68.3	24	68.6
Footage is subject to physical security measures	28	68.3	21	60.0
Access to the footage is documented	24	58.5	9	25.7
Access by external individuals, agencies, and organisations is governed by documented security procedures	22	53.7	7	20.0
Footage is subject to data encryption	7	17.1	2	5.7
Other	2	4.9	2	5.7
Footage is not managed formally	1	2.4	2	5.7
<b>Number of agencies</b>	<b>41</b>		<b>35</b>	

Base: Agencies that operated surveillance cameras (n=76)

Note: Numbers and percentages may add to more than sample totals since multiple responses were allowed

Source: Office of Economic and Statistical Research (2012), Use of Camera Surveillance (CCTV) Survey 2011.

## Appendix 4 – Considerations for future projects

Several issues for consideration were identified through respondent feedback and processing of survey data.

### Issue 1 – Microsoft Word version of survey

The CCTV survey encompassed large departments whose use and management of camera surveillance may be managed by multiple areas and staff members. As a result, a number of agencies requested a printable version of the questionnaire to send around within their agency to aid completion of the survey.

OESR created and sent a Microsoft Word version of the questionnaire to all agencies. This was done by importing the survey questions and instructions straight from the web into a Word document. Unfortunately, instructions on how to respond to each question may have been unclear when administered as a Word survey.

For example, one respondent pointed out that Q2.1 on the Word survey did not indicate that only one option could be chosen for each question. The web survey did not explicitly state this instruction as it was programmed to allow only one response option to be chosen.

If the agency contact responsible for inputting responses from the Word survey into the web survey received unusable responses to questions such as this, they would need to investigate and determine the correct response option, and thus needlessly invest more of their time to complete the survey.

### Recommendation 1

It is recommended that, in future, a Word version of the questionnaire be sent in the initial email invitation for the web survey.

Instructions for completing each question should be revised in light of the fact that some agencies will complete the Word survey and later input responses into the web survey. Restrictions on how many options can be chosen in each question, and instructions for any question skips, will need to be made explicit and clear in the Word survey to avoid respondent confusion.

### Issue 2 – Other specify for Q1.2

A number of agencies indicated in Q1.2 that they used cameras to monitor 'other areas' that were not catered for in the available response options. However, when asked to specify what these other areas were, two agencies responded with 'not applicable'. This may have occurred because agencies were asked to specify these other areas on the next page of the survey, and may not have realised this question (Q1.2h) related directly to their previous response (to Q1.2).

### Recommendation 2

The programming of the web survey does not allow respondents to enter both the number of cameras used to monitor 'other areas' and indicate what these other areas are on the same page. Bearing this limitation in mind, it is recommended that clearer instructions be included for Q1.2h *'Please specify the other areas in which cameras are used for the purpose of monitoring'*.

For example, "You indicated on the previous page that your agency uses cameras for the purpose of monitoring areas that were not in the list provided. Could you please specify these other areas in which cameras are used for the purpose of monitoring?"

### Issue 3 – Reporting total number and use of cameras

There appeared to be some confusion over how to correctly respond to Q1.2, with a number of illogical responses received which required confirmation and follow-up.

For example, four agencies originally indicated in Q1.1 that they operated surveillance cameras but when asked in Q1.2 to specify the total number of cameras operated, they responded with '0'. One agency reported a total of 123 cameras in operation, yet only specified for two of these cameras what their monitoring purpose was. Another agency (that operated 888 cameras) responded with '0' when asked to specify how many cameras were used for the purpose of monitoring (Q1.2a-f), despite being presented with the option to choose 'other areas'.

### Recommendation 3

It is recommended that agencies be asked to specify the total number of cameras operated by their agency before being asked to account for the purpose of each camera. Keeping these questions separate may reduce respondent confusion over the difference between the number of cameras operated and the number of camera purposes.

The survey should include clearer instructions for these questions (see example below), and be programmed to require the total number of uses of cameras to be greater than or equal to the total number of cameras in operation (as the purpose of each camera should be specified, and each camera can have more than one purpose). If the total number of uses is less than the number of cameras operated, respondents could be issued with an error message stating they have not accounted for the purpose of all cameras in operation.

Q1.2. How many cameras in total are operated by your agency? \_\_\_\_\_

Q1.3. How many cameras are used for the purpose of monitoring:

*Please specify the purpose of each camera your agency operates. Place a number in the box for each option that applies. If an option does not apply, please type '0'.*

*(NOTE: All purposes for each camera should be selected where there are multiple purposes. In other words, each camera can have more than one purpose.)*

Pedestrian traffic (eg. - malls, parks, public car parks, transport hubs) \_\_\_\_\_  
Vehicle traffic (eg. - on highways, roads, railway lines) \_\_\_\_\_  
etc.

### Issue 4 – Specifying government agencies in Q6.1

In Q6.1 agencies were asked whether they had an administrative arrangement with other organisations concerning access to their camera surveillance footage. One of the response options was 'Other government agencies, e.g. to the Queensland Police Service for law enforcement purposes (please specify)'. The majority (82.1%) of agencies who chose this option then specified that the arrangement was with the Queensland Police Service.

#### Recommendation 4

In future surveys, it is recommended that a separate response option be made available for arrangements with the Queensland Police Service. This would reduce the number of agencies that needed to manually type which government agency they had an administrative arrangement with, and the amount of recoding needed during the data cleaning stage.

## Appendix 5 – Agency Case Studies

---

### Background

In order to understand the use of camera surveillance systems, OIC reviewed a representative sample of agencies in-depth, by site visits, observations of the operations of the camera surveillance systems, review of agency documentation, and interviews with people using and running the systems. These in-depth reviews targeted the ways in which each agency adopted the requirements of the privacy principles when operating their camera surveillance systems.

The agencies reviewed in-depth were the Department of Communities, Townsville City Council, Logan City Council, Ipswich City Council and James Cook University.

### 1 The Department of Communities

#### 1.1 Overview

At the time of this review, the Department of Communities (**Department**) was a large and diverse government department. The Department's aim was to strengthen and protect the wellbeing of Queenslanders, particularly those who are vulnerable and most in need. The Department's service delivery areas included:

- Communities, Child Safety, Youth and Families
- Housing and Homelessness Services
- Disability and Community Care Services and Multicultural Affairs Queensland
- Aboriginal and Torres Strait Islander Services; and
- Sport and Recreation Services.

The Department employed approximately 10,029 people, and operated with a budget of \$4.4 bn. In the survey, the department reported holding 888 cameras. (Subsequent inquiries by the Department identified a further 70 cameras.)

Camera Locations (reported in survey response)	Numbers
Total	888

The Department was unable to break the figures down by location.

## 1.2 Survey Highlights

The survey found that the Department had strong local practices for managing camera surveillance, particularly with respect to data security (IPP4), as summarised below.

Survey highlights
<p>The Department has identified the need for policies but has just commenced the policy development work.</p> <p>The Department cited all the reasons identified in the survey as being reasons for the introduction of camera surveillance.</p> <p>Evidence the Department cited as being used to support the introduction of camera surveillance included an evaluation of existing camera surveillance and:</p> <p><i>Workplace security policies and procedures and critical incident reporting and risk assessment.</i></p> <p>Access to camera surveillance footage was reported as being handled under the RTI Act and IP Act. The Department also identified that their data security strategies included that individuals could only access footage if authorised to do so, that any access of footage was documented, and that footage was subject to physical security measures, for example, kept in locked storage. Department staff, particularly in Child Safety Service Centres, could view live footage on strategically placed monitors.</p> <p>The Department confirmed that footage could be released to QPS, stating:</p> <p><i>In relation to question 6.1, there is no overall administrative arrangement with other entities in place, however, information may be released to QPS for example under IPP 11.</i></p> <p>The Department was one of only 9 agencies (20.9% of the 43 agencies actively informing the community) which reported it advised the public how to get access to camera surveillance footage.</p>

However, the policy framework for operating the camera surveillance systems had not been considered from an agency-wide perspective, and as a result, there were procedures which were not formalised (for example, procedures governing disclosure of footage to other agencies).

The Department had a formidable array of detailed documents describing the technical specifications for camera surveillance systems, but very little documented policy or

procedure around the administration of the camera surveillance systems. Following the survey, the Department identified that this was an area needing further work, and established the 'CCTV Stakeholder group' chaired by the Information Champion, to develop policy and guidelines for the operation of camera surveillance. A guideline about the use of camera surveillance was in development. The Department expected that once this guideline was complete, the current standards for facilities design would be amended to incorporate the requirements of the camera surveillance guideline. The development of a new electronic document management system would similarly take the camera surveillance guideline into account.

### 1.3 Documentation of Policies and Procedures

Review of documents provided to this review	
Number of policy areas covered by documented policies, procedures or guidelines	Five policy areas covered out of twelve.
Overall quality of documents, in terms of inclusion of privacy considerations	Generally, documents were well structured but did not incorporate any mention of privacy issues.
Review Comments	
The Department had very detailed documentation describing the technical specifications for the cameras and the camera surveillance system, and specifications for facilities management. The documents did not address policy issues relating to privacy or the adoption of the privacy principles. In their survey responses, the Department advised that the policy development work had just commenced.	

### 1.4 Site visits

The review team visited the Brisbane Youth Detention Centre (237 cameras – the largest single installation of cameras) and the Ipswich South Child Safety Service Centre 'the CSSC' (8 cameras – which was representative of most Child Service Safety Centres).

#### Brisbane Youth Detention Centre

The Brisbane Youth Detention Centre had surveillance cameras on the perimeters of the facility, public pathways, some common areas and within rooms. There was prominently

displayed signage at these locations. Privacy within rooms was limited and variable. Some rooms had modesty screens in front of showers and toilets, and some did not. Residents were able to ask for cameras to be turned off while they used the shower or toilet. Residents were reported as being very aware of the surveillance and showed a degree of resentment about the surveillance through frequent attempts to damage the camera, obscure the image or lower the quality of the recorded images.

The camera footage was monitored from central monitoring rooms: one for the whole facility which could view footage from all of the cameras; and one in each residential block which could view footage for cameras in that block. The purpose for the cameras was to reinforce the security of the premises and for the protection of detainees and Centre staff. The cameras monitored the security of the perimeter and assisted in ensuring the safety of residents and staff, as part of a general safety strategy which relied primarily on staff. As a secondary purpose, the cameras could be used to safeguard property, for example, to identify when items were thrown over the perimeter fence.

The camera surveillance system could be used to identify areas or incidents that would require a rapid response. The system could also be used by staff to intensively monitor detainees who may be at risk of self harm. Preventive monitoring was generally done in person, for example, residents who might be at risk of self-harm were monitored in person by staff.

Camera surveillance footage was over-written at least every 30 days, and sometimes sooner, depending on whether or not the amount of recorded footage exceeded storage capacity. Recorded footage could only be accessed by two people, and was not accessible from the main central monitoring room.

Recorded footage was downloaded and provided to other agencies such as the QPS, the Crime and Misconduct Commission, the Ethical Standards Unit within the Department of Communities, internal auditors and the Commission for Children, Young People and the Child Guardian. When footage was disclosed, a receipt was obtained and the disclosure would be recorded in an audit log.

#### *The Ipswich South Child Safety Service Centre (CSSC)*

The Ipswich South CSSC had cameras located in the public lobby, carpark and in the interview rooms. There was prominent signage in these areas to advise people of the camera surveillance. The camera footage could be viewed on monitors mounted in the

general office area, so that any disturbances, for example in the interview rooms, could be observed, and the police alerted. Audio recording additionally occurred in the primary interview room. If they did view an incident where someone was at risk, the CSSC staff had instructions not to intervene themselves in the incident, but to dial 000 and obtain help from the police.

Staff reported that given the time that might elapse between staff noticing an incident and making a report, or between the report of an incident and the police response, the cameras were not seen as preventive. (Even if the police response was rapid they might not arrive in time to prevent escalation of violence, which might occur momentarily.) Rather, the cameras were seen as primarily providing a general deterrent and a record of incidents that could assist in any subsequent investigation of the incidents.

Recordings of the footage could be retrieved from a computer in a locked server room, to which four people had access. The recordings were kept for 30 days and then over-written.

Copies of the footage were disclosed to other people, for example the QPS, at an estimated frequency of one to four times per annum. On receipt of a request, the footage was viewed by CSSC staff to ascertain whether or not the cameras had captured any relevant information. The footage was released only on receipt of a subpoena or application made under the RTI Act, and with the approval of the Manager of the CSSC. Any release of footage was recorded on a standard form.

A copy of any footage provided to the QPS was kept by the CSSC, and if it contained the personal information of a client, the copy was kept on the client's file.

The CSSC maintained a user manual for the camera surveillance system. The manual was technically focussed, for example, described how to use the cameras, and did not deal with procedural issues, for example, how to take privacy considerations into account when deciding whether or not footage should be disclosed to the QPS. The staff induction manual was being reviewed and is to include information about the use of the camera surveillance.

### 1.5 Summary of Findings

Camera surveillance in the Department had been designed thoughtfully with very specific purposes in mind and operated carefully by the people immediately responsible for each

system.<sup>71</sup> In particular, local operations were designed and operated with data security in mind. Further work could be done by the Department to develop an overall strategy that built privacy considerations into office refurbishment standards, administrative policy and procedures for operating camera surveillance systems and the disclosure of camera surveillance footage to other agencies, for example, the QPS.

In responding to the draft report, the Department of Communities stated that it is committed to the good management of personal information collected by camera surveillance in accordance with the IP Act, *Public Records Act 2002* and associated information standards relating to record keeping and information security. The department provided OIC with information about its plans to address each of the recommendations in the report.

A significant initiative is the development of a *CCTV Privacy Guide* for staff to communicate the various obligations and issues arising from handling personal information collected by camera surveillance across the department. The *CCTV Privacy Guide* will outline obligations in respect of collection, storage, security, access, use and disclosure of personal information captured by camera surveillance systems and assist staff in adopting practices that comply with the IPPs. The department stated it would provide a draft copy of the *CCTV Privacy Guide* to OIC for comment prior to final approval by the department.

Comments were sought from the Department of Justice and Attorney-General, following a transfer of responsibility for the Brisbane Youth Detention Centre from the Department of Communities to the Department of Justice and Attorney-General during the course of the review. The Department of Justice and Attorney-General stated that the report accurately reflected the usage of cameras surveillance in the Brisbane Youth Detention Centre, and provided comments on the context of that usage, which have been taken into account in the final report.

---

<sup>71</sup> As an example, the Ipswich CSSC had blanketed areas under camera surveillance with clear but obviously 'home-made' notification signs. This was a result of staff initiative rather than a governance policy.

## 2 Ipswich City Council

### 2.1 Overview

The Ipswich City Council's services include provision of infrastructure, community services, water, waste management, recreation facilities and access to energy and technology. Council employs approximately 1200 staff and operates with a budget of approximately \$340 m. Council reported operating 420 surveillance cameras.

Camera Locations (reported in survey response)	Numbers
Other areas. The agency reported: <i>Safe City Monitoring 201 cameras, Asset Protection 219 cameras (includes monitoring of illegal dumping of rubbish and illegal use of parks and reserves.)</i>	420
<b>Total</b>	<b>420</b>

### 2.2 Survey Highlights

Council reported incorporation of a range of privacy considerations in the design and operation of the camera surveillance system.

Survey highlights
<p>The agency reported policies in all eight areas identified in the survey.</p> <p>As an additional type of usage, the agency reported:</p> <p><i>During 2011 Floods, system was used to monitor flood levels with areas covered by cameras.</i></p> <p>Evidence used to support the introduction of camera surveillance included research into the effectiveness of cameras, a privacy impact assessment and evaluations of existing security cameras.</p> <p>Data security included the use of documented procedures, an access log and physical security measures.</p> <p>As an additional comment, the agency stated:</p> <p><i>Standard policy takes personal privacy seriously. Standard procedure states an operator does not focus on an individual for longer than necessary. Known as the 2 second rule, the camera only focuses on a person for no longer than to obtain sufficient information to identify that person for possible later identification if required for investigative purposes.</i></p>

### 2.3 Documentation of Policies and Procedures

Review of documents provided to this review	
Number of policy areas covered by documented policies, procedures or guidelines	Two policy areas covered out of twelve.
Overall quality of documents, in terms of inclusion of privacy considerations	The documents that were in place were excellent from a privacy perspective.
Review Comments	
<p>The Ipswich City Council's documentation provided to this review was of a very high standard, particularly the Personal Information Digest No. 7, which listed the Council's personal information holdings, the Privacy Statement, and the forms used for requests for footage and recording release of footage to third parties, for example, QPS. These forms are a model which could be adopted by other agencies.</p> <p>Policy documentation about the decision to implement camera surveillance, the policies for the overall operation of the system, documents about staff training and policies for making decisions about future expansion of the system were not provided to this review.</p>	

### 2.4 Site visits

The review team visited Council's monitoring room and inspected locations of cameras used in surveillance.

There were two camera surveillance systems in operation in Ipswich: the Safe City Program system; and a system for the security of Council facilities. This review focussed on the Safe City Program system, which operated approximately 200 cameras. These cameras were observed in a number of locations in Ipswich's central business district. There was limited public signage concerning the cameras.

The Safe City Program developed from a partnership between Council and QPS with the express aims of preventing incidents and having a rapid response to incidents. The cameras were monitored by two security officers 24 hours a day, seven days a week. If an incident occurred or was seen as being imminent, the security officers contacted QPS

to view the situation first hand, for example at the QPS monitor at Yamanto, so that QPS could assess the situation and if necessary, send police officers to the scene immediately. The QPS monitor was matched to one of approximately 130 screens displaying Council's camera surveillance footage. The security officers could select the screen in question from the 130 screens, and place that camera's view on the monitor matched to the QPS monitor, so that QPS could view the relevant image.

The Safe City Monitoring system was operated by proprietary software, deliberately written to be incompatible with popular operating systems for data security purposes. The system was not connected to the internet, with one minor exception.<sup>72</sup> This software generated real time statistics about the usage of the system, which were reported monthly to Council. These statistics included reports on arrests known to have arisen from Safe City Monitoring, police infringement notices (tickets) known to have been issued as a result of Safe City Monitoring and calls to police by Safe City Monitoring to alert them to incidents or to situations which appear to be potential incidents. These statistics showed a clear pattern of prevention and prosecution.<sup>73</sup> Safe City Monitoring provided two examples of crime prevention, one involving the prevention of a rape, and the other prevention of an escalation of violent confrontation between two groups of young people.

Footage was recorded across several file servers, and retained for 14 days. Even with this limited retention of footage, the storage requirements to retain the images were substantial – 78 terabytes of data storage were required.<sup>74</sup>

Copies of the footage could only be extracted with the proprietary software. If QPS requested a copy of recorded footage, the file had to be extracted and viewed by the management of Safe City Monitoring to ensure it contained the information sought. If so, the image, an extract of the software needed to view that particular file and a copy of the file in an open format were burnt onto a disc and watermarked with relevant information about the file. The request was logged, the file viewed by QPS to ensure it was correct and a receipt collected from QPS for the disc. Safe City Program deleted copies of any files. After 14 days, Safe City Program retained no record of the footage.

This was a significant privacy failing of an otherwise exemplary system. Notwithstanding the Council's obligations under the *Public Records Act 2002* (see earlier discussion on this

---

<sup>72</sup> The exception is that when Windows needs updating, a technician is brought in to connect to the internet to update Windows, under the supervision of Safe City Program management.

<sup>73</sup> The exact statistics and other details of the system have been treated as confidential for the purposes of this report.

<sup>74</sup> A terabyte is 1024 gigabytes.

point), IPP11(2) obligates an agency to 'include with the document' a record of disclosure for law enforcement purposes. While Council made a note of the disclosure on the audit log, it kept no 'document' to which these notes could be referenced.

The Safe City Program had other strategies designed to protect privacy. One was the 'two second rule', which required security officers to zoom in on individual's faces for no longer than the two second necessary for identification of the individual. After two seconds, standard operating procedure for security officers was to zoom the image back out. Security officers were themselves subject to camera surveillance, and called to account if standard operating procedures, such as the two second rule, were not followed.

Safe City Monitoring contracted the monitoring function to a private sector security firm and provided specific training to the firm's security officers on the Safe City Monitoring system.

The training manual was detailed, and contained a section specifically dealing with privacy. Security officers were required to sign a Confidentiality Agreement, which reinforced the importance of privacy, confidentiality and data security.

As a final point, at a late stage in the review the media reported the use of the Safe City Monitoring system to identify drivers parking illegally in parking bays set aside for people with a disability. OIC contacted the Ipswich City Council to obtain further information about the incident. Ipswich City Council advised that the cameras had been used for this purpose, as part of a pilot program commenced to assess the value of using the camera system for other functions. All of the security systems had remained intact during the pilot. The program was not taken up once the pilot program had concluded.

This is arguably an example of 'function creep' where an agency's use of personal information is subsequently expanded for other purposes. While the privacy principles allow for new or alternate uses – and in particular IPP10 provides for a range of secondary uses – careful consideration should be given to incorporating privacy protection into the new use. This example shows that there can be negative public perception if the 'new' uses have not been adequately communicated.

## 2.5 Summary of Findings

In many ways, the Ipswich City Council Safe City Monitoring system was a model system. Privacy considerations were built into the development of the system and its operation.

There were two points of concern.

IPP11(2) *Personal information* requires that when a 'document' containing personal information is provided to another agency for 'law enforcement purposes' the disclosing agency must include a note of the provision with the document. This requirement was not followed sufficiently in Ipswich City Council's case. Footage copied for disclosure to another agency – most usually QPS - was deleted at the end of its 14 day lifespan regardless. Not only did this result in the Ipswich City Council having no record of what it disclosed but also this limited an individual's capacity to discover the nature of any of their personal information which had been disclosed to another agency.

This concern was mitigated by the meticulous log kept of the disclosure, and the fact that this footage should be available from the recipient of the footage, usually QPS. The review team was advised that Council contacted Queensland State Archives to obtain advice on the retention of camera surveillance footage.

Better signage in proximity to cameras would improve compliance with IPP2, and would add to the deterrence effect of the cameras.

These can be addressed through implementation of the recommendations in this report.

Ipswich City Council reviewed the draft report and made two minor suggestions to improve accuracy, which have been incorporated into the final report.



### 3 *James Cook University*

#### 3.1 Overview

Operating primarily out of Townsville and Cairns, James Cook University has approximately 20,000 domestic and international students, undertaking undergraduate and postgraduate courses in the Arts, Business, Creative Arts, Education, Engineering, Law, Medicine and Health Sciences, Science, Information Technology or Social Sciences. This review focussed on the largest campuses at Townsville and Cairns, where James Cook University reported having 231 surveillance cameras.

Camera Locations (reported directly to review) <sup>75</sup>	Numbers
Within government buildings	148
Precinct or immediate surroundings of a government building	83
<b>Total</b>	<b>231</b>

#### 3.2 Survey Highlights

Survey responses were not submitted.

#### 3.3 Documentation of Policies and Procedures

Review of documents provided to this review	
Number of policy areas covered by documented policies, procedures or guidelines	Two policy areas covered out of twelve.
Overall quality of documents, in terms of inclusion of privacy considerations	Generally, documents were well structured but did not incorporate any mention of privacy issues.
Review Comments	
James Cook University essentially did not have any relevant documentation for the implementation, operation or ongoing expansion of the camera surveillance system.	

The University had a well-structured approach to policy development and management in general, including a policy template, a policy library and management responsibilities

<sup>75</sup> Locations were apportioned into these categories by the review team, based on specific locations provided for each individual camera. Cameras at access doors, pathways and walkways were treated as being in a building precinct, and the remainder were treated as being within government buildings.

clearly delineated for different policy areas. This framework could be amended to ensure that privacy is a consideration when policies are being developed, that privacy considerations are included in the template and that privacy considerations are listed among the management responsibilities.

#### 3.4 Site visit

The review team visited the Townsville campus of James Cook University, and viewed the locations of cameras, the monitoring station and interviewed a number of people involved in the operation of the camera surveillance system.

The cameras were generally in public thoroughfares or laboratories - most notably the computer laboratories - and were relatively clearly signed.

The cameras were largely under the control of the security team, who operated from a central monitoring office and viewed camera footage on six screens in real time. The camera surveillance system was part of a suite of security strategies. Together with an alarm system for open or unsecured doors, the cameras assisted security in identifying and responding to incidents. The university campus has a student bar with inevitable crowd management concerns. While camera surveillance operates in the bar area, it was noted that most effective means of minimising adverse incidents was not the cameras but rather a cooperative partnership from campus security staff and police officers on site at relevant times. The security officers have also provided an escort service for protection, for example, traversing the campus at night.

The security staff have initiated many of their own privacy protections. One example was to erect a screen between the publicly accessible areas of the security office and the camera monitors. This build ensured that visitors to the office could not view the live footage.

The cameras were motion sensitive, and recorded footage when triggered by movement. Recordings over-wrote previously recorded footage, once the storage for camera footage was at capacity. Recorded footage could be retained for as little as two days or as much as ten days, depending on the extent of movement within the camera's view and therefore the speed with which the volume of recorded footage reached the storage capacity.

Recorded footage was disclosed to other agencies on request, for example, QPS. The request had to be made formally, and in the case of QPS, the QPrime reference number was requested to verify that the request was made pursuant to a law enforcement activity.

### 3.5 Summary of Findings

The camera surveillance system at James Cook University was operating in a way consistent with the privacy principles due in large part to its practical management by its immediate operators and managers. Again in large part, these practices and procedures were not documented at a local or corporate level. The system is accordingly vulnerable to staff changes. A policy and procedure framework needed to be developed and documented to ensure that the system itself was robust and that the privacy principles had been properly considered and incorporated into the future design and operating parameters of the system.

In response to the draft report provided to it, James Cook University stated that the report clearly reflected the information obtained during the site visit to the University, and would be of use to the University for any further action required to comply with the privacy principles in the *Information Privacy Act 2009* (Qld).



## 4 Logan City Council

### 4.1 Overview

Logan City Council provides local government services to Logan, the ward adjoining Brisbane to the south, with a budget of \$320 m and a staffing complement of approximately 1400 people. Council reported operating 538 surveillance cameras.

Camera Locations (reported in survey response)	Numbers
Within government buildings	108
Precinct or immediate surroundings of a government building	72
Pedestrian traffic areas	333
Vehicle traffic areas	25
<b>Total</b>	<b>538</b>

### 4.2 Survey Highlights

Survey highlights
<p>The agency has identified the need for further policies concerning camera surveillance.</p> <p>The Council reported using the cameras for all the reasons identified by the survey, and added two other uses:</p> <p><i>Confirming loads crossing the weigh bridge and for training purposes.</i></p> <p>Council reported using a range of methods to inform their decision to implement surveillance cameras, including a privacy impact assessment, and added:</p> <p><i>Staff and Public Safety; Council and Police crime statistics; Liquor Act; previous experiences at other locations.</i></p> <p>In the section on Disclosure of the Camera Surveillance Footage, agencies were asked which organisations they had an administrative arrangement with concerning access to camera surveillance footage. Logan City Council reported formal administrative arrangements for the release of footage:</p> <p><i>Libraries Policy, Formal memorandum of understanding between Council and Queensland Police Service and written formal procedures regarding footage release.</i></p> <p>Council uses two private contractors and states that the contractors are bound to the privacy principles in a written service contract.</p>

#### 4.3 Documentation of Policies and Procedures

Review of documents provided to this review	
Number of policy areas covered by documented policies, procedures or guidelines	Nine policy areas covered out of twelve.
Overall quality of documents, in terms of inclusion of privacy considerations	Generally, documents incorporated consideration of privacy issues. There were opportunities for improvement in the documents.
Review Comments	
<p>Logan City Council had well documented decision making processes for the installation, operation and evaluation of the camera surveillance system.</p> <p>Privacy issues were generally not incorporated in documents relating to policy decisions, for example, decisions to expand the camera surveillance systems. A test of the policy relating to the website showed that not all aspects of the policies had been implemented.</p> <p>The documents describing the day to day operations of the camera surveillance included privacy considerations. These could be updated and improved to reflect fully the requirements of the IP Act.</p>	

#### 4.4 Site visits

The review team visited the Logan City Council, its monitoring room and inspected camera surveillance at the Logan Entertainment Centre and the Logan Central Library.

The majority of cameras fell under the Community Services Branch's Safety Camera Program, which aimed to improve public safety, particularly at identified 'hotspots', for example high traffic areas which also had a higher crime rate compared to other places within the ward. Originally, there had been a second aim of improving security for businesses, and businesses had been encouraged to buy and maintain equipment in partnership with Council for this purpose. This aim was discontinued.

The cameras were monitored by a contractor's security officer, who advised police once an incident was under way, to facilitate a rapid response. The security officer viewed a feed from Council cameras and from cameras operated by Queensland Rail.

Queensland Rail footage was recorded and managed by Queensland Rail. Council recorded footage from Council cameras, and this was stored in a room separate from the monitoring room, which was accessible to four people. Cameras at the Entertainment Centre and Library sent footage to standalone computers which retained recorded footage for a limited period of time.

While the camera systems which monitored potential crime 'hotspots' were well considered, lesser consideration had been given to the cameras in the libraries and the Entertainment Centre. In the latter venue, cameras were legislatively required in the bar area but appeared to have little value beyond this legislative compliance. Cameras were located in areas and purposes that were not well defined. Interactions with these systems consisted of little more than maintenance of hardware.<sup>76</sup>

As with other organisations, Council had not assessed the camera surveillance system to clarify its reasons for having some cameras and the effectiveness and value obtained from others. The assessment could be an opportunity for the development of policies and procedures for continuing operation, maintenance and potential expansion of the camera surveillance system, one that incorporated the requirements of the IP Act as a matter of course.

One notable privacy protection employed by Council was to digitally mask footage capturing private property or sensitive areas – such as toilet block windows. In response to an inquiry Council stated that the owners of the relevant private property were informed that no footage would be captured in the Council's surveillance of their general area.

Requests for footage were made initially verbally, so that the security officer could view the footage to establish whether or not the information sought had been captured or retained. If the footage contained the information sought, a formal written application was made to the Manager of the Community Services Branch, or the local manager of the facility. The footage was copied onto a disc and released by a formal process.

---

<sup>76</sup> In one instance, the relevant Manager stated that he didn't know why the cameras were surveilling a particular area and what purpose could be served by the surveillance but that the cameras had been relatively recently upgraded regardless.

Copies of the released footage were kept with other Council records, except in the case of the Entertainment Centre, which deleted all footage after 28 days. This practice needed to be reviewed against the requirements of IPP11(2) under the IP Act, the *Liquor Act 1992* and the *Public Records Act 2002* .

#### 4.5 Summary of Findings

Logan Council had a well considered approach to camera surveillance, which had been thoroughly documented. This would be improved by incorporating explicit consideration of the privacy principles into the design and operation of the camera surveillance system, and ensuring that practices are consistent across Council facilities. For example, Council policies and procedures need to incorporate legislatively compliant provisions for retention of records and for individuals to access personal information held by Council.

Logan City Council was sent the draft report for its response. Detailed comments were received from the Community Services Branch. These comments were taken into account in the final report.

## 5 Townsville City Council

### 5.1 Overview

Townsville City Council provides local government to Townsville, aiming for a progressive and sustainable community. Council employs approximately 1700 staff and operates with a budget of \$380 m. Council reported having 172 cameras, of which 72 are part of the public safety system, located in hotspots with a primary aim of public safety. The remainder of the cameras are for a range of purposes, for example, monitoring environmental protection at landfill or water treatment sites, or for Council building or staff security and safety purposes. The original records of the reasons for establishing the system could not be located for this review.

Camera Locations (reported in survey response)	Numbers
Within government buildings	18
Precinct or immediate surroundings of a government building	55
Pedestrian traffic areas	88
Other areas, for example, galleries	11
<b>Total</b>	<b>172</b>

### 5.2 Survey Highlights

Survey highlights
Council reported having policies in place for seven of the policy areas identified in the survey and is developing a policy for retention and disposal of footage.
Public safety, crime prevention and crime enforcement were Council's stated reasons for introducing camera surveillance. Council did not report the evidence that was used to support this decision.
Council reported the use of password protection and an access log to protect the security of the camera surveillance footage.
Council reported an established procedure for QPS to access camera surveillance footage.

### 5.3 Documentation of Policies and Procedures

Documents were provided to this review as requested, and as summarised below.

Review of documents provided to this review	
Number of policy areas covered by documented policies, procedures or guidelines	Ten policy areas covered out of twelve.
Overall quality of documents, in terms of inclusion of privacy considerations	The documents provided a thorough policy framework, which is yet to be populated with all the identified policies and is yet to include a full set of privacy considerations.
Review Comments	
Most of the policy issues for Council as a whole were identified in one document: the <i>CCTV Knowledge Companion</i> . This document was an internal technology support document and was not intended for greater council or as a policy statement. It identified several policy areas needing further development, for example, CCTV policy, the CCTV maintenance contract, and the Memorandum of Understanding with the Queensland Police Service.	

During the site visit, further documents were identified by operational staff as being relevant to the review and these were provided to the reviewers. These documents were developed for local purposes and were not necessarily formally endorsed as Council policy or procedures. These included documents describing policies and procedures for the operation of specific camera surveillance systems, draft memoranda of understanding with QPS for disclosure of camera footage, a sample of the log of requests for camera footage and decisions about the requests, and a needs assessment procedure for determining whether or not cameras should be installed.

These policies and procedures for the camera surveillance system were detailed and comprehensive in terms of the needs of the operational area, and demonstrated care with the security of camera surveillance footage and disclosure of footage. Similarly, the draft memoranda of understanding with QPS, and the forms drafted for use by QPS when requesting material demonstrated adoption of privacy considerations in the disclosure of camera footage to QPS. The log of requests was detailed and a clear record of requests, decisions and reasons for the decisions. The needs assessment was also detailed but did

not incorporate privacy considerations. Overall, these operational level documents demonstrated careful thinking about issues of substance.

#### 5.4 Site visits

The review team inspected the monitoring station for the cameras in the Townsville City Council central administration building and in the monitoring room at the Garbutt Operations Centre.

Cameras were located in public streets, particularly 'hotspots', and in libraries, stadiums and waste management transfer stations. Signs were provided in the general vicinity of the cameras, but not in proximity to each camera.

The system was originally established over ten years ago. Records about the exact commencement of the system and the reasons for the installation of surveillance cameras could not be located. Interviewees advised that part of the initial impetus was the availability of federal funding to install cameras, and this was renewed recently to enable replacement of the equipment. Interviewees advised that the original system included real time monitoring of the surveillance cameras, and the monitoring function was co-located with a Police Beat to facilitate both preventive and rapid response measures to be taken. The real time monitoring and co-location with the police have both discontinued. The remaining vestiges of this system are the presence of a viewing monitor on QPS premises and the continued operation of the cameras themselves.

Over time, there have been other changes to the policies and procedures for operating the system and to the circumstances surrounding the current cameras which have affected their functionality:

- Some of the camera locations were selected some time ago, and over time, issues about the suitability of the camera placement have arisen. For example, the view from some cameras has become obscured by the growth of foliage in front of the camera, or as part of routine maintenance, when the camera has been re-situated, it has been sited on a post which partially obscures the view.
- Some of the cameras were selected with the capacity to be remotely directed, both for tracking across a field of view and zooming in to view images close up (Pan to Zoom (PTZ) cameras). These cameras were designed to be part of a camera surveillance system that was constantly monitored. The cameras are no longer monitored, and so the PTZ cameras now operate with automatic touring, that is,

the cameras move according to a pre-set, automated pattern. The constant mobility of the lens means that these cameras wear out and need greater maintenance than fixed cameras, and the automated movement means that the camera is frequently focussed away from places at the time that incidents occur, and so they do not capture the footage necessary to assist in investigating the incidents.

The log of requests for footage demonstrated the impact of issues with camera location and the automatic touring. In the extract of the request log provided to this review (96 requests for footage, between 12 July 2011 and 21 February 2012, all of which were from QPS), 55 out of 96 requests (57%) were refused. Of the refusals, nearly half were refused because the camera was not focussed on the place where the incident occurred at the time of the incident (24 out of 55 refused requests, 44%). The other major categories of reasons for refusal similarly reflected operational limitations of the camera surveillance system. 11 requests (20%) were refused because there was no camera in the area, 9 requests (16%) were refused because no footage was found and 6 requests were refused because the camera was not operational.

The process for making requests followed a relatively robust standardised practice. Requests for footage received from QPS had to be made using a written application form, and generally, a QPrime number was required to associate the request with a law enforcement activity (8 out of the 96 QPS requests did not record a QPrime number). Requests were generally made by constables. All other requests were treated as an application under either the RTI Act or IP Act. QPS had a video monitor on which they could view footage, but copies of footage had to be obtained from Council. QPS identified the incident time and location, and Council staff searched the footage to ascertain whether or not any relevant record existed. If a record existed, Council staff obtained a formal written request from QPS, cut the footage and copied it to disc, and provided QPS with a copy, together with a certificate as to the admissibility of the evidence in accordance with section 95 of the *Evidence Act 1977*. A file copy of any footage burned to disc and disclosed was saved on computer and retained indefinitely, as there was no disposal schedule for records of camera surveillance. A number of interviewees mentioned past efforts by Council to establish a Memorandum of Understanding with QPS to formalise these arrangements. While relatively comprehensive Memoranda of Understanding were

drafted, QPS declined to sign the memoranda. Corporate Governance advised that there was no current intention to enter into a Memorandum of Understanding with QPS.

The overall camera surveillance system was managed in a piecemeal way. Council defined roles and responsibilities for different business units to manage different activities associated with the camera surveillance system in *Principle 4878232 CCTV Custodianship*. Requests for footage and provision of copies of the footage were handled by Corporate Governance, who also dealt with any applications made under the RTI Act or IP Act. The officer responsible had the unique capacity to view monitors in real time, and review footage. The purchase, installation and maintenance of the cameras was done by a branch within Knowledge Management. The decisions about where cameras might be located in any future expansion of the system were made by Community Services. Cameras could also be monitored by Property Services. In fact, Property Services employed people who held qualifications in security monitoring and they had the best quality and most number of monitor screens, but their primary responsibility was not to monitor the cameras. Property Services' role in the camera surveillance system appeared to be to occasionally work with Corporate Governance from time to time to assist the relevant officer in reviewing footage and identifying whether or not any relevant recordings existed, and if so, which parts of the recording were relevant. Organisational policy and procedures were handled by a separate branch within Corporate Governance. This spread of responsibilities meant that although roles were clear, there was no one point of responsibility within Council for the operational integrity of the camera surveillance system. Interviewees advised that a meeting was called in response to this review, and if continued on a regular basis, the attendees at this meeting could coordinate the operation of the system.

Despite the well defined roles in planning, implementing and administering the camera surveillance system and the existing potential within Property Services, there is no live or retrospective monitoring of the cameras by Council staff. Council did not identify a Council function which used the cameras. Rather the cameras existed because of a perceived community expectation that Council would install and operate the cameras. In practical terms, and this has limited efficacy as detailed above, the almost exclusive 'use' the cameras were put to was in providing an occasional visual record for QPS' use in prosecuting an incident after it had occurred.

## 5.5 Summary of Findings

Townsville City Council had an established system of camera surveillance, the parameters of which had changed over time. The origins of the system were no longer clear, and it was not possible to assess whether or not the original system was set up appropriately. It was clear that the method of operation had changed significantly. For example, it was reported to this review that the system used to work beside real time monitoring and a close working relationship with QPS to prevent unlawful activity. Neither real time monitoring nor the close link to QPS to prevent unlawful activity remained.

However, a number of aspects of the previous system had been retained. These were no longer matched effectively to the new operating framework.

These aspects included:


- the deployment of cameras to locations which were not effective in capturing images of relevance because 'hotspots' had shifted
- the use of types of cameras which did not reliably capture footage of interest because they operated on automatic touring instead of being under the direct control of an operator monitoring the camera in real time
- replacement of cameras in locations where the view was obscured because of changes over time, for example, the growth of foliage in front of the camera
- the practice of giving QPS a single monitor and the capacity to direct which camera featured on their monitor, even though QPS no longer made use of this direct access and instead called on Council staff to identify and copy footage to investigate unlawful activity after it had occurred; and
- the dispersion of responsibility for the system across Council so that elements of the policy framework for the system were not coordinated.

In collecting personal information through camera surveillance, Council needed a clear reason for camera surveillance directly related to a function or activity of the agency (IPP1), and needed to ensure that the personal information collected was relevant for this purpose, was complete and up to date (IPP3). Council needed to review the camera surveillance system to clarify its reasons for having the system, and then establish a framework of policies and procedures for expansion, maintenance and operation of the system that reflect the requirements of the IP Act.

In its response to the report, Townsville City Council generally agreed that the report reflected their situation. They advised that they are currently in the planning phase of a number of initiatives including policy and procedure development, training and a review of practices. They also made specific comments on the report, which have been taken into account in the final report. They agreed specifically with the finding that aspects of the previous system were no longer matched to the new operating framework, and hoped that the recommendations may assist any evaluation of the Council's use of surveillance systems.



## Appendix 6 – Ipswich City Council Request Form



IPSWICH CITY COUNCIL  
**CCTV Footage Release**

**Requesting Officer's Name:**

**Job Title:**  **Work Unit:**

**Phone:**  **Email:**

**Signature:**  **Date of Request:**

**CCTV Footage Requested:**

**Location:**

**Time:**  **Date/Image Number:**   
(Image number is the incident date)

**Reason for Request:**

- What is being investigated (i.e. offence particulars), at least in broad terms;
- Why the information is necessary for the investigation; and
- Any law requiring or authorising Ipswich City Council to provide the information.

Ipswich City Council will consider this request and, depending on the sensitivity of the personal information that is requested, may require a warrant or other legal authority to be produced before release of any information. Ipswich City Council may release information if it is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health or welfare of an individual, or to public health, safety or welfare, or is satisfied on reasonable grounds that the disclosure is authorised or required under a law or that the disclosure of the information is necessary for use by a law enforcement agency under Information Privacy Principle 11(1)(e) of the *Information Privacy Act 2009* (Qld).

**Restriction on use of disclosure:** In accordance with Information Privacy Principle 11(3) in Schedule 3 of the *Information Privacy Act 2009* (Qld), Ipswich City Council requires that you must not use or disclose the information disclosed to you for a purpose other than for law enforcement or safety and welfare purposes.

The following information has been released under section 11(1)(c) (d) or (e) of Schedule 3 of the *Information Privacy Act 2009* (Qld).

**Details of documents released:**

**Internal Use Only:**

---

**Receiving Council Officer:**

**Date Received:**  **Signature:**

**RECEIVED:** Police /Applicant to complete below the line on collection

---

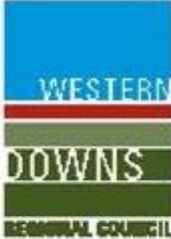
**Name:**  **Position:**

**Signature:**  **Date:**

Please submit to **Security Services Manager**, Safe City, Ipswich City Council via fax **(07) 3282 8054**



## Appendix 7 – Western Downs Regional Council collection notice



**IMPORTANT  
NOTICE**

Western Downs Regional Council is collecting your personal information on a closed circuit television system (CCTV) in this area. The personal information collected is being used for the purposes of public safety, crime prevention and detection. Your personal information will only be accessed by persons who have been authorised to do so. This information may be provided to the Queensland Police Service for law enforcement purposes. Your information will not be given to any other person or agency unless required by law. Your personal information is handled in accordance with the Information Privacy Act 2009.

Enquiries in relation to this notice may be directed to Western Downs Regional Council by calling 1300 728 500.

OUR COMMUNITIES | OUR FUTURE

