Office of the Information Commissioner
Queensland

Camera surveillance and privacy – follow-up review

Review of agency adoption of recommendations made under the *Information Privacy Act 2009* (Qld)

Report No. 1 of 2015-16 to the Queensland Legislative Assembly

The Office of the Information Commissioner (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.

Copies of this report are available on our website at 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
Web www.oic.qld.gov.au

ISBN: 978-0-646-94918-5

December 2015

The Honourable Peter Wellington MP
Speaker of the Legislative Assembly
Parliament House
George Street
BRISBANE Q 4000

Dear Mister Speaker

I am pleased to present 'Camera surveillance and privacy – follow-up review: Review of agency adoption of recommendations made under 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

Rachael Rangihaeata
Information Commissioner

Table of Contents

Supplementary Material

(provided on OIC website at oic.qld.gov.au)

Information Privacy and Camera Surveillance Survey 2015 – Survey, Website Scan and Comparison Report

Information Privacy and Camera Surveillance Survey 2015 – De-identified Comments by Agencies

Information Privacy and Camera Surveillance Survey 2015 – Queensland State School Sector Survey Report

Open data set versions (csv) of the survey responses

1 Executive Summary

This is a follow-up report on Queensland government agency implementation of 15 recommendations about camera surveillance and privacy made by the Office of the Information Commissioner to the Queensland Parliament during 2012-13.

In 2012-13, the Office of the Information Commissioner reported on the extent to which camera surveillance systems were designed and operated with privacy considerations in mind as required by the *Information Privacy Act 2009* (Qld).

This follow-up review has found that progress has been made in implementing all the recommendations of the original review.

It was evident that agencies had made substantial progress in their ability to track the number and details of cameras. Agencies provided a range of information about the number and purpose of usage of fixed surveillance cameras to the follow-up review, including that agencies operated 32,230 fixed surveillance cameras in 2015, an increase of almost 60% compared to 2011, when agencies reported operating 20,310 cameras. The follow-up review noted a trend of existing camera installations increasing in size.

Generally, the follow-up review noted increased inclusion of privacy considerations in the governance of camera surveillance systems, compared to 2011. In 2015, 80% of agencies reported that they actively informed the community about their use of camera surveillance. Each privacy element had been addressed by around half of the agencies in their surveillance camera policies, procedures and practices.

There continue to be opportunities for improvement. In particular, agencies could do more to address data security practices, implement policies and procedures for dealing with requests for footage and use their websites to provide information to the public. The review noted over 4000 requests for footage had been received by agencies in the previous 12 months. Almost 75% of the agencies operating camera surveillance cameras reported receiving at least one request for footage. Only approximately 40% of agencies reported having policies and procedures fully implemented to manage requests for footage.

Agencies reviewed in-depth in the original review provided progress reports to the follow-up review. These agencies had made progress in implementing the recommendations. The Department of Communities, Child Safety and Disability Services in particular had implemented a comprehensive suite of policies and procedures that could be a useful resource for other agencies in developing their own policies and procedures.

2 Report Highlights

The number of fixed surveillance cameras has increased by 60%

Between 2011 and 2015 the number of fixed surveillance cameras reported as being used by Queensland government agencies increased from 20,310 to 32,230.

In 2015, approximately half of Queensland government agencies had a full set of policies for the security of camera surveillance footage.

Many agencies lack sufficient data security policies for handling footage

Agencies need a framework to manage requests for footage

In the past 12 months, Queensland government agencies received 4000 requests to access footage but only 40% of the agencies had a framework of policies and procedures to manage a request.

Of the agencies reporting the use of fixed camera surveillance, it was easy to find related information on their website for approximately one in five agencies.

Only 20% of agencies had easy to find information online about their use of camera surveillance

3 Background

3.1 Introduction

This is a report on the implementation of recommendations of an Office of the Information Commissioner (**OIC**)[1] report. This report, tabled in Parliament during 2012-2013, described the increasing use of camera surveillance by Queensland government agencies and the extent to which fixed camera surveillance systems were designed and operated with privacy considerations in mind, as required by the *Information Privacy Act 2009* (Qld) (**IP Act**):

- **Report to Parliament No. 2 of 2012/13 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) (**original review / report)**.

The original review / report:

- analysed the extent to which agencies complied with the prescribed requirements of the IP Act
- identified and reported on areas of good practice; and
- made recommendations to improve all agencies' compliance with the IP Act.

The report of this follow-up review (**follow-up review / report**) examines the extent of implementation of the original review / report recommendations.

3.2 Review Framework

The review was 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. 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.

[1] A list of acronyms is provided in Appendix 1.

3.3 Scope and objectives

This follow-up review examined the extent to which Queensland government agencies' implemented the 15 recommendations made in the original review / report regarding compliance with the privacy principles.

The privacy principles are:

- the Information Privacy Principles (**IPPs**) for all agencies, except the Department of Health and Hospital and Health Services, which are subject to equivalent principles in the National Privacy Principles (**NPPs**) that are better suited to health service providers
- section 33 IP Act, relating to transfer of personal information outside Australia; and
- sections 34 to 37 of the IP Act, relating to contracted service providers.

The 15 recommendations of the original report are provided in full in Appendix 2 and details of the privacy principles, including the Information Privacy Principles (**IPPs**) are provided in Appendix 3.

3.4 Assessment process

Evidence was gathered through the following processes:

a. a survey of agency camera surveillance implementation and use was repeated to enable a comparison over time – this is referred to throughout this report as the Information Privacy and Camera Surveillance Survey 2015 (**IPCS Survey 2015**)

b. a scan of agency websites was conducted to identify publicly-available information about agencies' use of camera surveillance and the privacy elements adopted in their operations of camera surveillance – this is referred to throughout this report as the Website Scan 2015; and

c. the following agencies reviewed in-depth in the original review were contacted for a progress report:

   - Department of Communities, Child Safety and Disability Services
   - Department of Justice and the Attorney-General[2]

[2] Following 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, part of the Department of Communities reviewed originally was transferred to the Department of Justice and the Attorney-General.

- Ipswich City Council
- James Cook University
- Logan City Council; and
- Townsville City Council.

3.5 Reporting Framework

Information gathered through the IPCS Survey 2015 and Website Scan 2015 was compiled using the same report structure as the original survey report provided by the Office of Economic and Statistical Research (OESR Survey 2011).[3] The repeated use of most of the content of the original survey enabled direct comparison of results between 2011 and 2015, and comparison of both of the agency's surveys with the independent findings of the 2015 Website Scan 2015. The consequent findings are summarised throughout this report, while a full statistical report will be published as supplementary material to this report on OIC's website.[4]

Information about the progress of agencies reviewed in-depth was obtained from multiple methods, including the IPCS Survey 2015 and Website Scan 2015. Progress reports provided by these agencies identified examples of good practice which have been included in this report.

[3] *Use of Camera Surveillance (CCTV), Survey 2011-12, Survey report prepared for the Office of the Information Commissioner*, 1/3/2012, Final Version, Office of Economic and Statistical Research. The survey was conducted in 2011 and the report produced and tabled in 2012.

[4] https://www.oic.qld.gov.au/

4 Privacy – A systemic issue

Privacy requirements

Prevalence of camera surveillance

In 2011, agencies reported operating 20,310 surveillance cameras. However, many agencies were not able to accurately report on the number of cameras operated due to the way in which cameras had been acquired. For example, within an agency, a series of small purchases of camera surveillance equipment and systems in individual business units would have aggregated into a significant property asset for the agency. Agencies that did not accurately know the size and distribution of their surveillance camera holdings would be similarly unable to comply with the attendant governance obligations and to minimise risks associated with their camera operations. The review recommended agencies consider mechanisms for accurately capturing the number of cameras they operated and other relevant details about the camera surveillance systems.

Recommendations

Recommendation One

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

Overview of progress

A component of the follow-up review was to ascertain the extent to which camera surveillance was being used by government agencies. This was compared to the extent of camera surveillance usage identified in the original review to assess the rate of growth of camera surveillance usage.

Although there has been a slight increase in the number of agencies operating fixed surveillance cameras, the most significant increase was in the number of cameras operated overall. There was a 58.7% increase from 20,310 fixed surveillance cameras reported as being operated by government agencies in 2011 to 32,230 cameras reported as being operated in 2015. However, it is noted that a proportion of this increase is

Overview of progress

attributed to cameras in schools, for which data is available for the first time in the IPCS Survey 2015.

The high response rate to the IPCS Survey 2015 (79.6% of agencies) and the clarity of agency responses indicated that many agencies had a system for tracking the number and details of surveillance cameras operated by the agency. However, in the absence of 40 agency responses and given receipt of incomplete responses regarding the number of cameras, OIC cannot make a finding regarding implementation across all government.

Having regard to the agencies who responded to this question, OIC considers good progress has been made in the implementation of Recommendation One.

4.1 Introduction

The original review examined:

- the extent to which camera surveillance was being used by government agencies
- differences in policies, procedures and practices between agencies that had large camera installations and agencies that had only a few cameras
- the degree of formalised policy documentation governing the systems; and
- the extent of corporate review of practices adopted on the ground.

This follow-up review conducted the IPCS Survey 2015 and Website Scan 2015 to revisit the findings and changes to the agencies' operation of camera surveillance, focusing on agencies' ability to track and report on the number and details of surveillance cameras operated by agencies.

4.2 Overall results

The IPCS Survey 2015 identified that there was an increase in the percentage of agencies reporting the use of camera surveillance from 63.3% in 2011 to 71.2% in 2015. This was linked to changes in the number of government agencies and internal structure within government agencies and a higher response rate in 2015.

The number of government-operated cameras increased significantly between 2011 and 2015, from 20,310 cameras reported as being operated in 2011 to 32,230 cameras reported

as being operated in 2015. The average number of cameras operated per agency increased from 267.2 cameras in 2011 to 309.9 cameras in 2015.

Just over three-quarters of the cameras (76.1% of cameras) were operated either by Queensland Government departments (38.6% of cameras) or local governments (37.5% of cameras), with the top five agencies operating 58.4% of all fixed surveillance cameras.

The distribution of cameras across agencies is depicted in Figure 1.

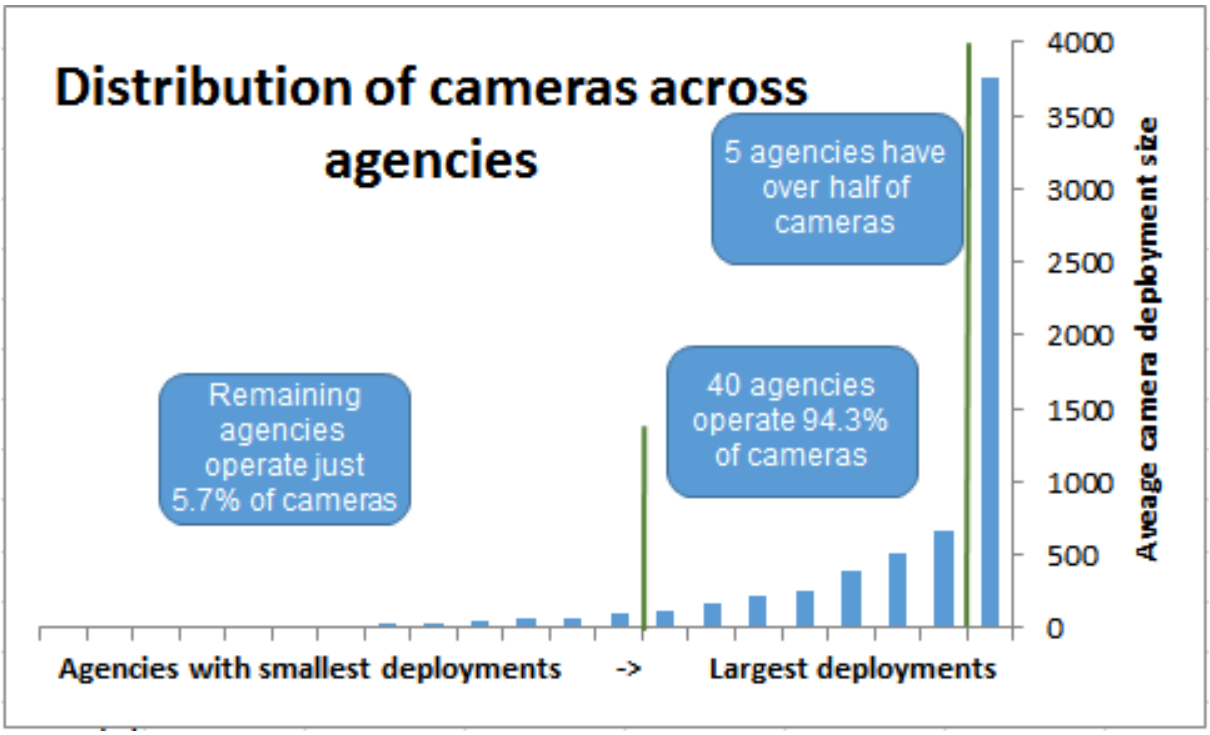

Figure 1 Distribution of cameras across agencies

Generally speaking, all agency holdings had grown larger, so that agency installations tended to be medium or large-sized and there were fewer small installations.

In 2015, 156 agencies responded to the IPCS Survey 2015 (a response rate of 79.6%). A notable and welcome result was that the Department of Education and Training was able to provide information about the operation of cameras within 1151 Queensland schools.

Overall, agencies that responded to the IPCS Survey 2015 answered over 95% of the applicable questions.

4.3 Findings regarding progress of implementation

The high response rate, the clarity regarding the numbers of cameras being operated and the thoroughness with which agencies completed the IPCS Survey 2015 indicated that government agencies were better placed now to accurately know the number and details of surveillance cameras operated by the agency.

However, a definitive count of the cameras operated by Queensland government agencies is still not known:

- 40 (20.4%) of agencies did not respond to the IPCS Survey 2015
- 14 agencies did not supply either the total number of cameras or a breakdown of the cameras including:
    - 7 agencies reporting they used surveillance cameras but did not supply the total number of cameras; and
    - 13 agencies did not supply a breakdown of the purpose for each camera, although seven of those 13 agencies provided a total number of cameras.

The shortfall in responses affected OIC's ability to assess implementation of Recommendation One.

The lack of responses or incomplete responses limited the potential to make a finding about the extent to which every government agency had implemented a system to track the number and details of surveillance cameras.

Overall, however, the improvement of responses both in terms of detail and number of responding agencies can be taken as an indication that agencies are better placed to report on the number of deployed cameras and the uses to which they are deployed, as recommended. This will have a beneficial flow-on effect in terms of a consistent application of the privacy principles to deployed cameras across the agency.

5 Information Privacy Principles 1 - 3 – Collection

Privacy requirements

IPP1 Collection of personal information (lawful and fair). *(similar to National Privacy Principle 1)* Agencies should only collect personal information which is necessary for one or more of the agencies' functions or services. The collection must not be unlawful or unfair.

IPP2 Collection of personal information (requested from individual). *(similar to National Privacy Principle 1)* Agencies need to take all reasonable steps to ensure an individual is generally aware of the reasons and authority for collecting personal information, and which other entities to which they would usually disclose the information.

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.

Recommendations

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.

Recommendations

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.

Overview of progress

The majority of agencies (83.3%) had at least one piece of information or evidence to support the introduction of the agency's fixed camera surveillance system.

In general, between 40% and 50% of agencies had implemented policies, procedures or practices to address the recommendations regarding:

- that their management of fixed camera surveillance aligned with the reasons for implementing it; and
- having procedures in place to ensure camera surveillance footage was complete and up-to-date.

The great majority of agencies (80%) advised the community about their use of camera surveillance, compared to just over half (56.6%) in 2011. The most popular method used to inform the community was by a notice in the general area where cameras were deployed.

Agencies under-used their websites in providing relevant information to the community about these policies, procedures and practices.

Implementation of these recommendations is in progress.

5.1 Introduction

An agency should be able to clearly articulate and communicate the direct relationship between the purpose for which camera surveillance is used and the agency's functions or activities. An agency should be able to point to information or evidence supporting the use of camera surveillance for that purpose. When an agency collects personal information from an individual, the agency must take reasonable steps to make the individual generally aware of the purpose for the collection, any lawful authority for the collection and anyone who routinely would receive this information from the agency. This information can be set out in written form in a 'collection notice'. The 'collection notice' for camera surveillance could be a sign posted in the vicinity of the camera which informs the community of the purpose for the surveillance. In addition agencies can provide information on their deployment of camera surveillance on their web-sites.

5.2 Overall results

Out of 108 agencies answering IPCS Survey 2015 questions regarding the information or evidence supporting the introduction of camera surveillance, 18 agencies (16.6% of respondents) reported they had not relied on any information or evidence or did not know what information or evidence was relied on to support introducing camera surveillance for the identified purpose. This was a slightly reduced percentage compared to 2011, where 21.1% of respondents did not rely on information or evidence or did not know what information or evidence was relied on to support the introduction of camera surveillance.

Of those agencies able to identify information or evidence supporting the introduction of camera surveillance, the most commonly cited information or evidence was general research into the effectiveness of camera surveillance (41.7% of agencies responding to this question) or an evaluation of the effectiveness of existing systems (41.7% of agencies responding to this question). Over half of the responding agencies (50.9% of agencies) also cited 'other' information or evidence, which was described in the comments as including a security review, crime and safety considerations, mandatory as agency fit-out, or responses to incidents. Privacy impact assessments were not commonly conducted for camera surveillance introductions or expansions in 2011 or 2015.

As part of their progress report in response to the follow-up review / report, the Logan City Council provided OIC with a copy of an operations manual for its camera surveillance

program.[5] The operations manual included a section on Accountability (section 6.6) which committed to independent evaluation of the camera surveillance system, and a section on Security and Privacy Impact Assessment (section 6.9) which committed to a privacy impact assessment prior to any expansion of the camera surveillance system, including the introduction of new cameras. This was a positive adoption of evidence-based decision making in the ongoing management of the camera surveillance system.

The specific responses that agencies provided as to their reasons for having camera surveillance were primarily public and staff safety, property protection and crime protection. These reasons were reflected throughout the responses and the comments.

In response to the IPCS Survey 2015, the majority of agencies reported having some documented policies and procedures governing the use of camera surveillance. One of the questions in the IPCS Survey 2015 dealt with the extent to which agencies ensured that the management of fixed camera surveillance footage was consistent with the reasons for implementing fixed camera surveillance. Almost half the agencies answering this question (48.6% of responding agencies) stated they ensured they managed cameras consistently with the reasons for having the cameras, and it was either done or at least recognised as an issue by 90 agencies (84.1% of responding agencies).

A comparison of the Website Scan 2015 and the IPCS Survey 2015 results showed that in general, agencies could make more use of their websites to notify the community about their policies, procedures and practices regarding fixed camera surveillance. Just over half of agencies which had reported the use of camera surveillance in the IPCS Survey 2015 also included information on their websites which made it clear that the agency operated camera surveillance (54.1% of agencies reporting the use of camera surveillance – see Figure 2).

[5] *Logan Safety Camera Program: Management and Operations Manual*, Logan City Council, (operations manual).

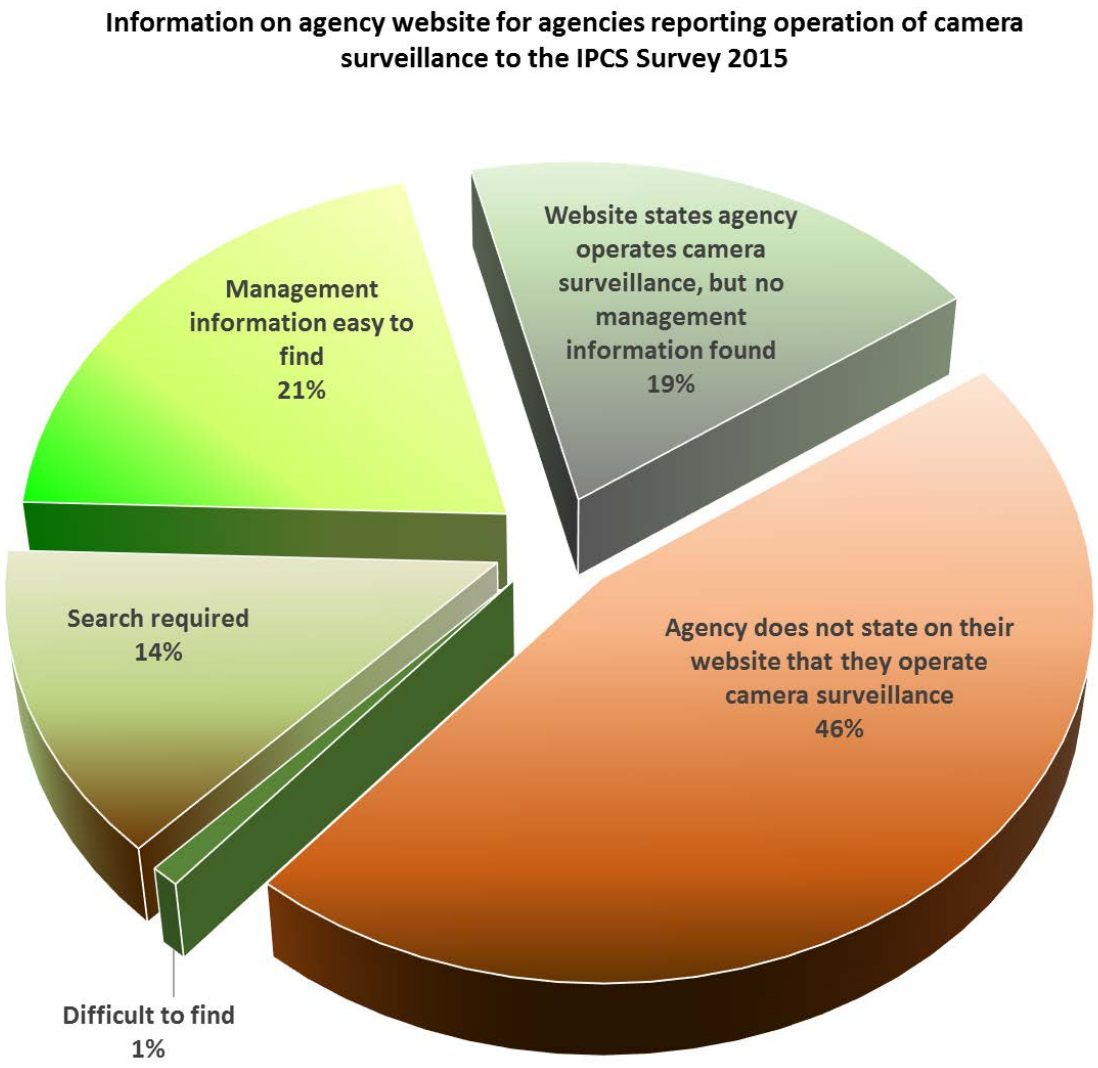

Figure 2 Agency use of websites to provide information about their use of camera surveillance

Even if there was information about the management of camera surveillance on an agency website, this information was not always easy to find. Of the agencies reporting the use of fixed camera surveillance in the IPCS Survey 2015, it was easy to find management information on the agency's website for less than one in five agencies (20.7%).

This review obtained information about each agency's purposes for using camera surveillance in a number of ways.

These reports differed. Agencies were likely to have consistently reflected in both the IPCS Survey 2015 and on their website the purposes of public and staff safety and property protection. Half of agencies that identified these reasons:

- crime prevention
- crime investigation and enforcement and
- increase public perception of safety;

had also made information on these reasons for camera surveillance available on their website. While agencies identified research, meeting public demand, managing traffic and responding to a trigger issue as reasons for installing camera surveillance in the IPCS Survey 2015, they did not provide this information to the public on their websites (see Figure 3).

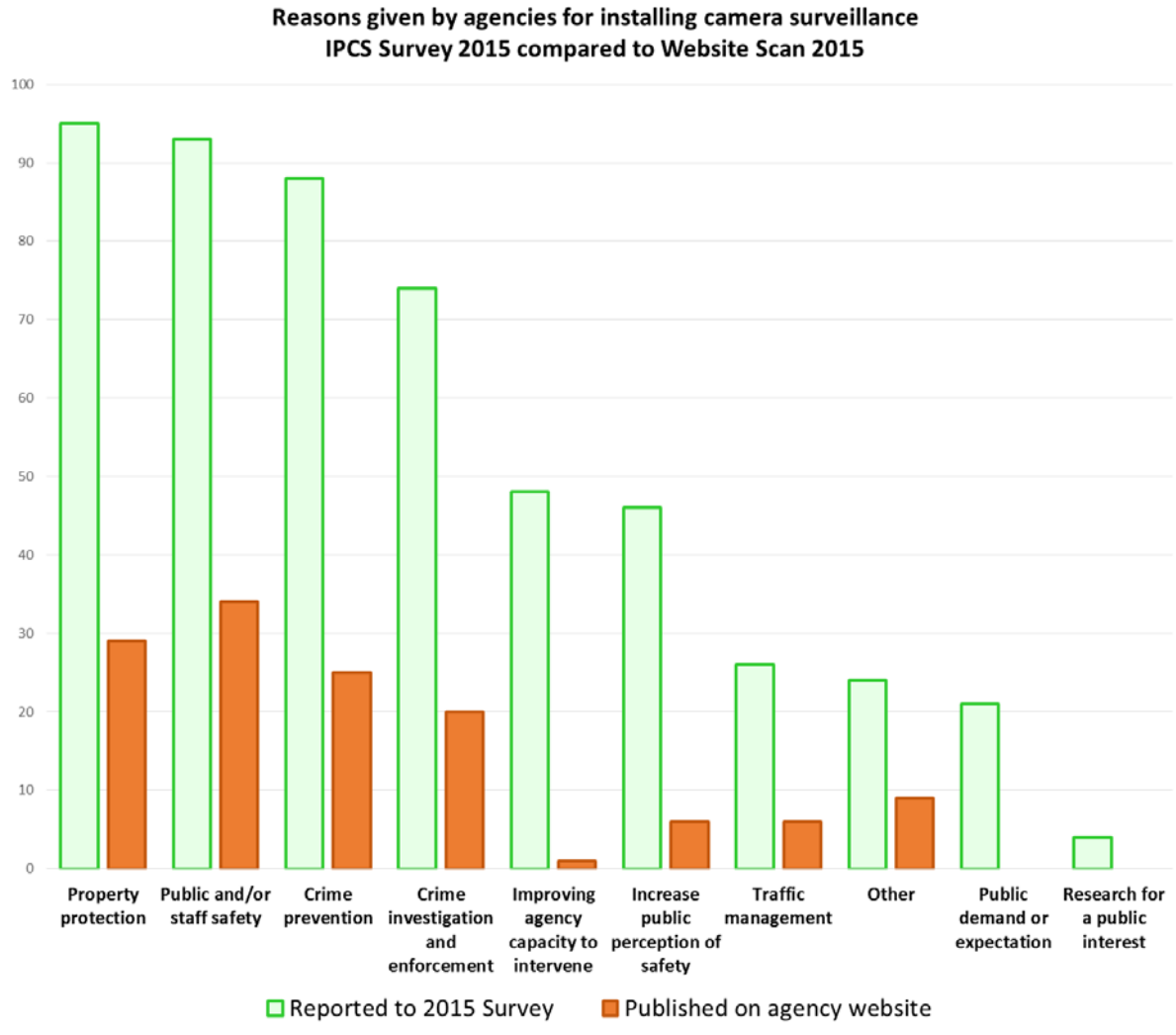

Figure 3 Reasons published on agency websites for having camera surveillance, for agencies reporting operation of camera surveillance to IPCS Survey 2015

Using camera surveillance for law enforcement

The use of camera surveillance for law enforcement purposes is reflected in the close relationship between some agencies – most notably, local governments – and the Queensland Police Service in the management of camera surveillance. This could create a possible confusion about management responsibility for the fixed camera surveillance system, including for the obligation to comply with the privacy principles. This comment provided to the IPCS Survey 2015 illustrates the potential blurring of responsibility and ownership of camera surveillance:

> *The installation of CCTV cameras is supported by the local Police based on their experience and results obtained in other communities. They are very keen to expand Council's existing network of cameras.*[6]

While the main external users of an agency's camera surveillance system may be the Queensland Police Service, at all times, the agency is responsible for the administration of the system including compliance with the obligations in the privacy principles. This includes the obligations arising out of disclosure to the Queensland Police Service. The Queensland Police Service is independently responsible for compliance in terms of its own dealings with camera surveillance footage.

A sizeable minority percentage of agencies (43%) reported having procedures in place to ensure camera surveillance footage was complete and up-to-date. Most agencies had recognised the need to do so (90 agencies, 84.1% of agencies responding to this question). Half of agencies that operated surveillance cameras had addressed in full in a documented policy or procedure the process for informing people about the fixed cameras (50.9%).

Agencies demonstrated awareness of the need to manage their use of camera surveillance so as to minimise privacy impacts. For example, agency comments in the IPCS Survey 2015 indicated that agencies had taken steps to manage privacy impacts of the possible capture of footage of residential property. Some agencies reported configuring or programming cameras to 'ensure there is no direct coverage of private premises or sensitive semi-public areas such as inside public toilets'. Other agencies use 'virtual privacy screening' through the camera to prevent capture of footage of residential property. Some agencies relied on another Government agency such as the Queensland Police Service

[6] Note that 'CCTV', the acronym for Closed-Circuit Television, was used interchangeably with camera surveillance at times.

(three agencies) or the Department of Transport and Main Roads (one agency) to manage this risk.

About 80% of all agencies reported advising the community about camera surveillance, usually by a sign in the general area where the cameras are used or in the immediate vicinity of the cameras. This was a significant increase compared to 2011, when 67.4% of the agencies responding to the OESR Survey 2011 reported having a notice in the general area of the cameras.

Half the agencies reported having policies and procedures for informing people about the fixed cameras. About a third of all agencies also published in a document a description of camera surveillance, mainly being the agencies operating larger numbers of cameras and with more policies and procedures about the camera surveillance system. There was no significant increase in the number of agencies notifying the community about their camera surveillance in a publicly accessible document between 2012 and 2015.

The Website Scan 2015 conducted by OIC confirmed that a relatively small percentage of agencies provided information on their websites to notify the community about camera surveillance. The majority of the information that was reported to IPCS Survey 2015 could have been made available to the community on agency websites.

5.3 Findings regarding progress of implementation

OIC found agencies had made good progress relating to:

- the evidence used to introduce camera surveillance
- the alignment between the operation of the camera surveillance system and the reasons for implementation
- agency practices to ensure currency and completeness of footage; and
- the notification to the community about the collection of the footage.

However, more progress could have been made by the majority of the agencies surveyed to fully implement appropriate policies, procedures and practices.

Comments made to the IPCS Survey 2015 suggested that there continued to be possible ambiguity of ownership and responsibility for camera surveillance between some agencies and the Queensland Police Service. It is important that each agency understands their respective obligations under the IP Act.

OIC also found that the majority of agencies were not making full use of their websites to provide information to the community about the operation of the camera surveillance systems.

Implementation of these recommendations is in progress.

6 Information Privacy Principle 4 – Data storage and security

Privacy requirements

IPP4 Storage and security of personal information. (*similar to National Privacy Principle 4)* Surveillance camera footage must be stored so that it is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.

Recommendations

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.

Overview of progress

Most agencies store camera surveillance footage on their own premises, protected by physical security measures, and required individuals to have authorisation to access the footage, or to have password protection for the footage.

This was the situation in 2011, and little has changed between 2011 and 2015. Additional data protection strategies have not been comprehensively adopted. Of concern is the increased percentage of agencies relying on informal management of camera surveillance footage.

OIC did not find that agencies had made much progress towards implementing this recommendation compared to the original review.

6.1 Introduction

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, but IPP4 has a broader applicability.[7]

6.2 Overall results

Agencies generally stored camera surveillance footage on their own premises (almost 90% of agencies), a situation in 2015 almost identical to that in 2011.

Agencies managed access to footage by limiting access to authorised individuals (83.5% of responding agencies), storing footage under password protection (68.8% of responding agencies) and protecting footage through physical security measures such as keeping footage in locked storage facilities (59.6% of responding agencies). These results were stable between 2011 and 2015.

Over one half of agencies that operated surveillance cameras had a documented policy or procedure in full for protecting camera surveillance footage against loss, unauthorised access, disclosure, modification or misuse (51.4%).

Agencies that operated higher numbers of surveillance cameras and with more privacy elements included in their policies and procedures also reported having implemented more formal management procedures than agencies with fewer cameras or fewer policies.

There were a small number of agencies who responded that they did not know how the footage was kept secure (1.8%) or thought that there were no formal procedures for keeping the footage secure (10.1%), an increase compared to 2011 when 3.9% of agencies reported footage was not managed formally.

As part of their progress report, the Department of Communities, Child Safety and Disability Services provided OIC with a copy of a procedure: '*Workplace Security*'. This included a dedicated section on the operation of CCTV, including procedures for retention and disposal of footage, notifying the public about the camera surveillance and the usage of the cameras.

[7] However, it remains an option for non-government agencies to adopt IS18 as practice.

OIC considered this to be a best practice procedure for ensuring camera surveillance was used properly and footage was protected against loss, unauthorised access, disclosure, modification or other misuse.

6.3 Findings regarding progress of implementation

The majority of agencies kept camera surveillance footage on their own premises and had at least one strategy for protecting this data. There was little change between 2011 and 2015.

Flaws in agency data protection strategies remain. For example, over 16% of agencies did not manage access to footage by requiring individuals to be authorised to access camera surveillance footage. The risk of loss, unauthorised access, disclosure, modification or misuse of footage has increased because a higher percentage of agencies were using informal strategies to manage data security.

Agencies have made limited progress in advancing the protection of data security.

7 Information Privacy Principle 5 – Individual can find footage

Privacy requirements

IPP5 Providing information about documents containing personal information. *(similar to National Privacy Principle 5)* 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.

Recommendations

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.

Overview of progress

These recommendations have been addressed in a very limited way.

In particular, agencies have under-used websites as a means of informing the community. While publishing information online about the currency of footage and the mechanism for obtaining that footage is a compliance issue, there is a practical benefit for both the agency and individuals to having an informed and focussed access request for footage.

7.1 Introduction

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.

7.2 Overall results

Almost half of the agencies reported that they had policies and procedures in place across their agency detailing how individuals could find out if there was any current camera surveillance footage of them (45 agencies, or 42.1% of agencies). Another 18 agencies (16.8% of agencies) reported they were developing these policies and procedures or had developed procedures for part of the agency.

However, agencies generally did not report that they were doing this by publishing a list of camera surveillance footage or contact details for enquiries, and the Website Scan 2015 found that agencies generally under-used their websites to provide relevant information.

Including camera surveillance footage as part of a list of personal information holdings had the lowest take-up of surveyed privacy items within policies across all agencies, by a significant margin. Only 12 agencies (11.3%) reported publishing a full list of fixed camera surveillance footage holdings, and 66 agencies (62.3%) reported this had not been done and had not been identified as a task that needed to be done. The Website Scan 2015 similarly found that of the agencies reporting to the IPCS Survey 2015 that they operated camera surveillance, 21 agencies (18.9%) published information about camera surveillance footage in an online list of personal information holdings.

Of the 23 agencies that either had published a list of holdings or were in progress towards publishing a list of holdings, 8 local governments and 9 agencies in the other agency sector accounted for the majority of agencies addressing this requirement. Two departments reported publishing or being in the process of publishing a list of holdings of fixed camera surveillance footage.

Agencies that stated they published a list of holdings of camera surveillance footage were almost twice as likely as other agencies to notify the community about surveillance in a publicly accessible document (58.3%).

Of the 88 agencies[8] that actively informed the community about camera surveillance, about a third reported including as part of that information:

- the name of the service and contact details (31 agencies, 36.0%)
- the process by which people could seek access to footage (29 agencies, 33.7%); and
- how long the footage was kept before overwriting or disposal (16 agencies, 18.6%).

The Website Scan 2015 found that 16 agencies provided information about holdings of fixed surveillance cameras on their websites, with an additional 14 agencies mentioning camera surveillance footage but providing no information. Of the 12 agencies that published some information about retaining camera surveillance footage, eight agencies published information about the retention period for camera surveillance footage.

As part of their progress report, the Department of Communities, Child Safety and Disability Services provided OIC with a copy of an information sheet titled '*Camera Surveillance Systems and Privacy – IPP5*', which provided a clearly set out description of the way in which the department applied the privacy principles in its operation of camera surveillance, and which provided information as to how community members could apply for copies of footage, make a complaint about the system or contact the department regarding camera surveillance. A copy of this information sheet is viewable online[9] and is also provided in Appendix 4, as it is a useful resource for other agencies when drafting their own information resources.

7.3 Findings regarding progress of implementation

In contrast to the amount of information that agencies provided about the cameras, agencies were much less informative about the camera surveillance footage, despite claiming that they provided this information to the public. Around one in ten agencies fully published information about the camera surveillance footage. Only 16 agencies provided information about the currency of the footage, with 13 agencies publishing this information online. A person seeking to contact an agency to find out if their image was captured or to obtain a copy of any captured images was assisted to do so online by around 30 agencies.

The result is that a person who wanted to conduct online research to find out for themselves whether or not their image might have been captured by camera surveillance would find it

[8] 88 agencies reported they actively informed the community about camera surveillance. Two of these agencies did not provide information to the survey about the type of information made publicly available.

[9] Viewed at https://www.communities.qld.gov.au/gateway/site-information/privacy on 27 November 2015.

difficult to get answers. They would also be unlikely to be able to find out for themselves whether or not the footage was still potentially available.

Three quarters (74.5%) of agencies reported receiving at least one request to access camera surveillance footage. For any agency dealing with requests for footage, publishing information online about the availability and currency of footage and how to obtain that footage is not only a simple compliance issue, it is a practical way to assist individuals to inform themselves before contacting an agency to request camera surveillance footage.

These recommendations have been addressed in a very limited way.

8 Information Privacy Principle 6 – Individual can access footage

Privacy requirements

IPP6 Access to documents containing personal information. *(similar to National Privacy Principle 6)* An individual must be able to access camera surveillance footage containing personal information about them if they ask for it.

Recommendations

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.

Overview of progress

This review did not examine agency practices for responding to requests for information, but instead focussed on implementation of systems to support the making of requests and appropriate agency responses to requests for camera surveillance footage.

Nearly 75% of agencies reported receiving in total around 4,000 requests for footage from individuals, other agencies and third parties in the last 12 months.

The high level of community interest in accessing video was not matched by commensurate mechanisms in the agency to enable the access requests. Overall, there is a dearth of policies, procedures and published information for individuals making requests and a corresponding lack of guidance for agency staff actioning the requests.

Implementation of these recommendations is in progress.

8.1 Introduction

IPP6 states that if an individual asks for access to camera surveillance footage containing images of them, the agency must give the individual access to that footage. IPP6 also states that it is discretionary for an agency to deal with access requests under its formal access application scheme. Under this scheme, access can be denied if there is a countervailing public interest to providing an individual with access to footage that captures their images.

OIC acknowledges that providing a third party with access to footage containing images and possibly sound of an individual raises privacy issues with respect to that individual. Because commonly camera surveillance footage can capture the images of multiple persons at any given time, dealing with an access request from just one of those persons under an administrative access scheme may not be appropriate.[10] While this follow-up review did not examine in depth, agencies' handling of access requests, anecdotally, OIC understands that agencies are routinely redacting the images of third parties in order to administratively release video footage.

Camera surveillance footage is a 'document' of an agency and entities can apply to access camera surveillance footage under the *Right to Information Act 2009* (RTI Act) and Chapter 3 of the IP Act.[11]

8.2 Overall results

The requirement that agencies provide documents on request in accordance with legislative requirements can be split into two steps: firstly that individuals are supported to make a request, and secondly that agency staff are supported to action the request appropriately.

82 agencies (74.5% of agencies) had received requests for footage from a range of requestors. 64 agencies provided information about the number of requests received, reporting receipt of approximately 4,000 requests in the previous twelve months. Over a quarter of the agencies receiving requests had received requests from individuals seeking to access footage of themselves (22 agencies). Most of these (86.4% of agencies receiving requests from individuals) were agencies with large holdings of cameras.

---

[10] OIC acknowledges the special case of footage released administratively to the Queensland Police Service where release is 'reasonably necessary' for a law enforcement function.

[11] 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.

42 agencies (39.3%) had a policy and 19 agencies (17.8%) were developing a policy or had a policy covering part of the agency as to how an individual could request or seek access to footage containing images of them. At least half of the agencies in each sector had a policy in full or part or were developing a policy. Departments, Universities and TAFEs were most likely to have a policy.

Generally speaking, each privacy element had been addressed by around half of the agencies in their surveillance camera policies, procedures and practices, including for example, for implementing administrative arrangements about disclosure of footage to other agencies or third parties (47 agencies, or 44.3% of agencies).

Compared to the total of 61 agencies (57.0% of agencies) with a policy or developing a policy for individuals' access to footage, only a third of agencies stated that they provided information to the public about the process whereby people could seek to access footage (33.7% of agencies). The Website Scan 2015 showed that few agencies made information on how to access camera surveillance footage available on the agency website (22.5% of agencies reporting having camera surveillance).

Overall the information provided online on how to access camera surveillance footage was accurate (25 out of 31 agencies providing information, or 80.6%), but detailed information was only provided by 16 agencies. Two agencies provided information on seeking access through legal representation or a subpoena but not through the IP Act, and four agencies provided information which contained inaccuracies.

In response to requests for copies of the footage, 45 agencies (42.1% of agencies) had policies and procedures for staff as to how to scan footage and extract material (24 agencies or 22.4% of agencies had addressed this in part or were developing policies and procedures).

These policies and procedures were not well complemented by staff training. The actual extent of training reported by agencies as being provided to staff about policies and procedures did not alter much between 2011 and 2015 (around 30% of agencies had training in place in both years), but there was greater recognition by agencies of the need for training (24.3% of agencies without training identified the need for training in 2015, compared to 10.5% in 2011).

8.3 Findings regarding progress of implementation

Agencies had not met the volume of requests with a matching degree of development of policies and procedures to manage these requests. Around three-quarters of agencies had received at least 4,000 requests in total over the previous 12 months for camera surveillance footage from individuals or others (74.5% of agencies). Overall, only around 40% of agencies had implemented policies and procedures for managing requests from individuals seeking access to footage of themselves, and 44% of agencies reported having administrative arrangements to deal with disclosure to other agencies or third parties. However, nine agencies received 80% of these requests. Six of these nine agencies had implemented policies and procedures for managing requests from individuals seeking access to footage of themselves, and seven of these nine agencies reported having administrative arrangements to deal with disclosure to other agencies or third parties

Given the number of agencies receiving requests for footage, provision of guidance to agency staff could be improved. Policies and procedures for staff to deal with requests by scanning footage or extracting material were in place for only 42.1% of agencies, and around 30% of agencies had fully implemented training to staff in agency policies and procedures.

Overall, agencies did not use their websites effectively to inform the public about their use of camera surveillance and the ways in which the camera surveillance systems operated, including how requests for footage could be made and how they would be processed.

Neither the IPCS Survey 2015 nor the Website Scan 2015 provided information as to the extent to which requests for footage were refused, addressed in full or addressed in part, for example, by redacting camera surveillance footage.

In summary, the review found that not all agencies had developed systems to enable individuals in making requests for footage and providing guidance to agency staff on how to respond to any requests.

Implementation of these recommendations is in progress.

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.

Recommendations

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.

Overview of progress

Although almost two-thirds of agencies either had or were developing policies and procedures governing the extraction of fixed camera surveillance footage relevant to a request, a comparison of 2011 and 2015 survey results suggested that little had changed.

There continue to be opportunities for improvement in the implementation of this recommendation.

9.1 Introduction

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

9.2 Overall results

In the original review / report, the key issue underpinning the recommendation was that agencies were spending significant amounts of time viewing footage to identify and extract material responsive to requests for footage from the Queensland Police Service. Agencies were recommended to review the way this was done and ensure the privacy principles were adopted. Agencies were asked about policies and procedures relevant to this issue in the

IPCS Survey 2015, and just under half reported having the relevant policies and procedures in place. If agencies reporting part implementation were included, around two-thirds of agencies reported either having or developing the relevant policies and procedures.

45 agencies (42.1% of responding agencies) had policies and procedures for how a staff member scans footage and extracts material in response to a request of copies of the footage, and 24 agencies (22.4% of responding agencies) were developing these policies and procedures or had policies and procedures for part of the agency, a total of 69 agencies (64.5% of responding agencies).

9.3 Findings regarding progress of implementation

Although two-thirds of agencies either had or were developing policies and procedures governing the extraction of material from fixed camera surveillance footage, a comparison of 2011 and 2015 survey results suggested that little had changed.

There continue to be opportunities for improvement in the implementation of this recommendation.

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

Privacy requirements

IPP10 Limits on use of personal information. (similar to NPP2) An agency might use camera surveillance footage for secondary purposes under certain circumstances such as: 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. (similar to NPP2) Camera surveillance footage may be disclosed to third parties under certain circumstances including: with the consent of the individuals concerned; to prevent serious threats to health, safety or welfare; for law enforcement; or for research purposes. Agencies commonly regularly disclose surveillance camera footage to the Queensland Police Service.

Recommendations

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.

Overview of progress

Around two-thirds of agencies had or were developing policies or procedures governing disclosure of camera surveillance footage, and were most likely to address factors such as disclosure when reasonably necessary for law enforcement, disclosure when the individual was aware the agency would usually disclose their personal information or disclosure where it was reasonably necessary for health and safety purposes.

Around half of the agencies operating surveillance cameras reported having administrative access arrangements. Nearly all of these arrangements were with other government agencies, primarily the Queensland Police Service. A significant majority of these arrangements (nearly 90%) operated in accordance with a formal document or procedures and (nearly 80%) required the requesting agency to complete a standardised form, which would assist the agency to comply with its privacy obligations for the disclosure of the camera surveillance footage.

Although these findings are positive, the recommendations were not adopted by all relevant agencies. Over all agencies, implementation of these recommendations is in progress.

10.1 Introduction

An agency can use camera surveillance footage for secondary purposes – such as training of staff - or disclose footage to other agencies if they comply with the criteria in IPPs 10 and 11 - for example, if they have the consent of the individuals concerned or the secondary use or disclosure is to prevent serious threats to health, safety or welfare for law enforcement activities; or for research purposes.

The most likely entity to which agencies might disclose surveillance footage would be to the Queensland Police Service for use in law enforcement activities. Agencies would usually cooperate with requests from law enforcement agencies such as the Queensland Police Service for access to surveillance camera footage.

10.2 Overall results

In response to the IPCS Survey 2015, 50 agencies (46.7% of responding agencies) stated that they had a policy or procedure for providing fixed camera surveillance footage to others and disclosure of camera surveillance footage, and 22 (20.6% of responding agencies) stated this was in development or had been developed for part of the agency.

45 agencies (42.5% of responding agencies) had policies and procedures governing the use and limits of use of fixed surveillance camera footage, particularly unanticipated use, and 21 agencies (19.8% of responding agencies) were developing these policies and procedures or had policies and procedures for part of the agency, a total of 66 agencies (62.3% of responding agencies).

The Website Scan 2015 identified 21 agencies which had information on managing camera surveillance published in online policies and procedures, and found differences in which the exemptions in the IPPs for secondary use and disclosure were addressed in agencies' policies and procedures.

Agencies which had an online policy and/or procedure that addressed camera surveillance were most likely to have detailed information on secondary use and disclosure for law enforcement purposes (12 agencies, 57.1%), for when the individual would have been aware the agency usually disclosed the information (11 agencies, 52.4%) and for health and safety purposes (11 agencies, 52.4%).

Agencies were least likely to address use and disclosure for research or statistical analysis (6 agencies had some information, 28.6%) and marketing (5 agencies, 23.8%).

Agencies overall had the same level of transparency across multiple items, such that an agency with detailed information in one area was more likely to have detailed information across multiple other areas. Five agencies - all local governments - provided detailed information on their websites covering off each of the exemptions available for secondary use and disclosure of their camera surveillance footage.

Nearly all of the agencies reported in the IPCS Survey 2015 that the fixed surveillance camera footage was only used for the relevant purpose for which it was originally commissioned. Six agencies reported using the footage for another purpose, and those agencies also reported that they had considered and addressed the privacy implications of the secondary use.

Few agencies which identified they used camera surveillance on the IPCS Survey 2015 provided information on their secondary use and disclosure of personal information on their websites (3.6% to 16.2%). These agencies were most likely to provide information on secondary use and disclosure where necessary for law enforcement (16.2%), where authorised or required under a law (14.4%), where necessary for life, health, safety or welfare (14.4%) or where the secondary use was directly related to the original purpose (14.4%).

Managing disclosure of information to the Queensland Police Service continued to be a significant issue in 2015, with analysis of comments to the IPCS Survey 2015 indicating that the Queensland Police Service had accessed or requested access to camera surveillance footage from 80.0% of the agencies that had received a request (64 agencies).

Disclosure of camera surveillance footage to others was managed in a structured way by some agencies. Over half of government agencies that operated surveillance cameras (52.3%) reported having an administrative arrangement with another entity concerning access to the agency's camera surveillance footage. This showed no change from 2011. Almost all of these agencies (98.2%) reported that they had administrative arrangements with other government agencies to access their camera surveillance footage. This was consistent across agency types, camera deployment sizes and levels of policy implementation. Only six agencies reported having an administrative arrangement with an organisation which was not a government agency. The comments showed that the most common entity with which government agencies had an administrative arrangement with was the Queensland Police Service.

Where there was an administrative access arrangement, 87.9% of agencies reported to the IPCS Survey 2015 that it was done in accordance with a formal written agreement or established procedures, and 78.6% of agencies reported that access required completion of a standardised request form.

As part of their progress report, the Department of Communities, Child Safety and Disability Services provided OIC with a copy of factsheets regarding the use of camera surveillance recordings as records and managing digital photographs and recordings as records. These factsheets specifically referenced the information privacy principles as part of their in-house procedures for use and disclosure of camera surveillance footage. The factsheets stressed the importance of ensuring records were accurate, up-to-date and complete, that disclosure had to be in accordance with Information Privacy Principle 11 and that consent forms were

required if digital recordings were contemplated to be used in departmental publications. The inclusion of these steps in the policies and procedures provided clear guidance to ensure compliance with the privacy principles in the management of camera surveillance.

Since 2011, the Logan City Council has formalised their policies and procedures documenting how camera surveillance supports the reduction and prevention of crime and which includes an operations manual setting out in detail their liaisons with the Queensland Police Service.

10.3 Findings regarding progress of implementation

Around two-thirds of agencies reported to the IPCS Survey 2015 that they had or were developing policies or procedures governing secondary use or disclosure of camera surveillance footage. The Website Scan 2015 indicated that these were most likely to have detailed information on secondary use and disclosure for law enforcement purposes, for when the individual would have been aware the agency usually disclosed the information or for health and safety purposes.

Around half of the agencies operating surveillance cameras reported having administrative access arrangements for disclosing their camera surveillance footage with external entities. Nearly all of these arrangements were with other government agencies, primarily the Queensland Police Service. A significant majority of these arrangements (nearly 90%) operated in accordance with a formal document or procedures and (nearly 80%) required the requesting agency to complete a standardised form, which would promote consideration of privacy in the disclosure of the camera surveillance footage.

Although these findings are positive, the recommendations were not adopted by all relevant agencies. Looking across all agencies, implementation of these recommendations is still in progress.

11 Privacy Principles – Contractors

Privacy requirements

In the main, the privacy principles only apply to Queensland government agencies. They do not ordinarily 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 governments), the agency is obligated under chapter 2, part 4 of the IP Act to take all reasonable efforts 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.

Recommendations

Recommendation Fourteen

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

Overview of progress

The majority of agencies using private contractors since the commencement of the IP Act had bound the private contractors to the privacy principles.

There were three agencies who had not bound the private contractors to the privacy principles, and so were possibly non-compliant with the IP Act. Implementation of this recommendation is in progress.

11.1 Introduction

Agencies are required to take all reasonable efforts to bind contracted service providers to the privacy principles.

11.2 Overall results

Over a quarter (29.1%) of agencies that operated camera surveillance systems indicated that their surveillance systems were operated in part or fully by a private sector contractor. Through the comments, agencies identified 18 different private contractors operating, installing and/or maintaining government agencies' surveillance systems.

Overall, 60% of agencies using private contractors to operate their camera surveillance systems entered into contracts for this service from the introduction of the IP Act. Of these, 15 agencies (83.3%) bound the contracted service provider to the privacy principles and 3 agencies (16.7%) had not bound the contracted service provider to the privacy principles.

The IP Act provides a measure of flexibility for agencies to use or disclose information in permitted circumstances. Once bound, the contracted service provider can also utilise these flexibilities. While not required under the IP Act, an agency may wish to clearly detail how the contracted service provider is to comply with specific privacy obligations. Fewer specific measures were covered in contracts in 2015 compared to 2011.

Safety and security of footage, access to footage and disclosure of footage to third parties were the measures most likely to be explicitly covered in contracts with contracted service providers (60.0% each). Less than half of agencies explicitly covered retention and disposal of footage (46.7%) or secondary use of footage, that is, use of the footage for a purpose other than that for which the camera was initially installed and operated (40.0%). Six agencies (40.0%) while binding the contracted service provider to the privacy principles in general did not include any privacy-specific contractual measures.

11.3 Findings regarding progress of implementation

The majority of agencies using private contractors since the commencement of the IP Act (15 out of 18 agencies, 83.3%) had bound the private contractors to the privacy principles.

There were three agencies who had not bound the private contractors to the privacy principles, and so were possibly non-compliant with the IP Act.

Implementation of this recommendation is in progress.

12 Privacy Principles – Overseas transfer of information

Privacy requirements

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

This protection covers all online activity including websites, overseas-based cloud services,[12] off-shore data storage and processing and online tools such as survey applications and social media programs.

Recommendations

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.

Overview of progress

Less than half of the agencies reporting transfer of camera footage overseas also reported having policies and procedures to ensure that any camera surveillance footage transferred overseas, for example placed on the internet, ensure that the transfer complies with the obligation in section 33 of the IP Act.

Implementation of this recommendation is in progress.

[12] *Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.* (definition from Webopedia, viewed at http://www.webopedia.com/TERM/C/cloud_services.html on 30 September 2015.)

12.1 Introduction

The obligations in section 33 will arise if camera surveillance footage is transferred overseas, for example, if the footage is stored overseas or is posted on a web-site or social media site.[13] Consideration as to the applicability of this section would necessarily need to occur if the agency used overseas cloud service providers[14] or other off-shore storage facilities.

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

12.2 Overall results

The majority of agencies (90.9%) did not report transferring their camera footage outside Australia: 8.2% of agencies reported they had camera footage available on the internet, 1.8% stored their camera footage offshore, and 0.9% transferred their camera footage outside Australia by other means.

Of the ten agencies which reported transferring their camera footage outside of Australia, nine provided information on their consideration of the relevant privacy obligations regarding this transfer. Four of these agencies (44.4%) had a policy and/or procedure to ensure compliance with the privacy obligations surrounding transfer of personal information outside Australia implemented in part or full. 29 additional agencies also addressed this in their policies and/or procedures, even though they reported they did not transfer camera footage overseas.

12.3 Findings regarding progress of implementation

Less than half of the agencies reporting transfer of camera footage overseas also reported having policies and procedures to ensure that any camera surveillance footage transferred overseas, for example placed on the internet, complied with the 'transfer out of Australia obligations' in section 33 of the IP Act.

Implementation of this recommendation is in progress.

[13] 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.

[14] Defined in Appendix 1.

13 Conclusion

The clear finding of this follow-up review was that across the board, agencies using surveillance cameras have significantly increased the size of their camera installations since 2011, without necessarily developing corresponding policies, procedures and practices incorporating privacy considerations. Further improvement is required across all sectors of Queensland government agencies to address compliance requirements and meet community expectations about safeguards for handling personal information.

Progress has been made in implementing the 15 recommendations, and some individual agencies have made significant progress. The review identified good examples of policies, procedures and practices for operating camera surveillance compliant with the obligations in the privacy principles.

However, the progress made by government agencies was variable. In general, around half of the agencies did not have sufficient policies, procedures and practices concerning their use of camera surveillance, and the mechanism by which members of the community could find out more about the agency camera surveillance system or specifically, information that would enable them to access camera surveillance footage. In particular, agencies could make much better use of their web-sites to provide this information.

The review included a survey sent to all agencies, which concluded with optional questions about the use of mobile cameras. Agencies were very responsive to the optional questions, revealing that the expansion of fixed security cameras had been matched by a concomitant expansion of mobile camera systems. Agencies reported that they were adopting new surveillance technologies, such as body-worn cameras and drones, to assist in discharging their functions and responsibilities.

The expansion of government agencies' use of existing and their adoption of new technologies means that privacy will become an increasingly important consideration for agencies, not least, in order to foster community confidence in the effective deployment of these systems.

OIC will continue to provide advice and assistance regarding agency adoption of the privacy principles in their use of monitoring technologies to encourage and support agencies to build and operate the most effective and trustworthy monitoring systems, meet community expectations and improve privacy compliance and practices.

APPENDICES

Appendix 1 – Acronyms

CCTV	Closed-Circuit Television
Cloud	Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. (definition from Webopedia, viewed at http://www.webopedia.com/TERM/C/cloud_services.html)
Follow-up review / report	This report of the follow-up review and the follow-up review
IP	Information Privacy
IP Act	*Information Privacy Act 2009* (Qld)
IPCS Survey 2015	*Information Privacy and Camera Surveillance Survey*, 2015, conducted by the Office of the Information Commissioner
IPP	Information Privacy Principle
IS18	Information Standard 18: Information Security
NPP	National Privacy Principle
OESR	Office of Economic and Statistical Research, now the Office of the Queensland Government Statistician (OQGS)
OESR Survey 2011	*Use of Camera Surveillance (CCTV), Survey 2011-12, Survey report prepared for the Office of the Information Commissioner*, 1/3/2012, Final Version, Office of Economic and Statistical Research.
OIC	Office of the Information Commissioner
OQGS	The Office of the Queensland Government Statistician, formerly the Office of Economic and Statistical Research (OESR)
Original review / report	The report of the original review and the original review
RTI	Right to Information
RTI Act	*Right to Information Act 2009* (Qld)
Website Scan 2015	A scan of all agency websites conducted by the Office of the Information Commissioner in 2015

Appendix 2 – List of Recommendations of Original Review Report

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.

It is recommended that:-

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.

It is recommended that:-

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.

Appendix 3 – The Privacy Principles

33 Transfer of personal information outside Australia

An agency may transfer an individual's personal information to an entity outside Australia only if—

(a) the individual agrees to the transfer; or

(b) the transfer is authorised or required under a law; or

(c) the agency is satisfied on reasonable grounds that the transfer 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) 2 or more of the following apply—

(i) the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is a health agency, the NPPs;

(ii) the transfer is necessary for the performance of the agency's functions in relation to the individual;

(iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;

(iv) the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs.

34 Meaning of *service arrangement*

(1) In this Act, a service arrangement is a contract or other arrangement entered into after the commencement of this section under which an entity other than an agency (the contracted service provider) agrees or otherwise arranges with an agency (the contracting agency) to provide services.

(2) For subsection (1)—

(a) the services must be for the purposes of the performance of 1 or more of the contracting agency's functions; and

(b) the services must be provided either—

(i) directly to the contracting agency; or

(ii) to another entity on the contracting agency's behalf; and

(c) the contracted service provider must not be in the capacity of employee of the contracting agency in providing the services.

35 Binding a contracted service provider to privacy principles

(1) An agency entering into a service arrangement must take all reasonable steps to ensure that the contracted service provider is required to comply with part 1 or 2 and part 3, as if it were the agency, in relation to the discharge of its obligations under the arrangement.

(2) However, the agency must comply with subsection (1) only if—

(a) the contracted service provider will in any way deal with personal information for the contracting agency; or

(b) the provision of services under the arrangement will involve—

(i) the transfer of personal information to the contracting agency; or

(ii) the provision of services to a third party for the contracting agency.

(3) The agency is not required to comply with subsection (1) if—

(a) the contracted service provider is to receive funding from the contracting agency; and

(b) the contracted service provider will not collect personal information for the contracting agency; and

(c) the contracted service provider will not receive any personal information from the contracting agency for the purposes of discharging its obligations; and

(d) the contracted service provider will not be required to give the contracting agency any personal information it collects in discharging its obligations.

(4) Subsections (1) to (3) are not intended to limit what may be provided for in a service arrangement about the contracted service provider's collection, storage, handling, accessing, amendment, management, transfer, use or disclosure of personal information, whether or not the contracted service provider is a bound contracted service provider.

36 Bound contracted service provider to comply with privacy principles

(1) A bound contracted service provider under a service arrangement must comply with part 1 or 2 and part 3 in relation to the discharge of its obligations under the arrangement as if it were the entity that is the contracting agency.

(2) The requirement to comply under subsection (1) continues to apply to the bound contracted service provider in relation to personal information it continues to hold after its obligations under the service arrangement otherwise end.

(3) A bound contracted service provider's compliance with part 1 or 2 and part 3 may be enforced under this Act as if it were an agency.

(4) Subsections (1) to (3) are not intended to prevent a service arrangement from including a requirement for the contracted service provider to comply with all or part of the privacy principles even though this part does not require that the service arrangement include the requirement.

37 Contracting agency to comply with privacy principles if contracted service provider not bound

(1) This section applies if a contracted service provider under a service arrangement is not a bound contracted service provider because the contracting agency under the service arrangement did not take the steps required of it under section 35.

(2) The obligations that would attach to the contracted service provider if it were a bound contracted service provider attach instead to the contracting agency under the arrangement.

The Information Privacy Principles (IPPs)

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 4 – Example of good information resource

Department of Communities, Child Safety and Disability Services

Camera Surveillance Systems and Privacy – IPP5

The Department of Communities, Child Safety and Disability Services (the department) is committed to ensuring that personal information collected by surveillance camera systems is handled in accordance with the Information Privacy Principles (IPPs) contained in the *Information Privacy Act 2009* (Qld).

Purpose

Surveillance camera systems are used by the department to monitor and record activity for a range of purposes including, providing a safe and secure environment for departmental staff, clients and the general public, as well as for property protection and crime prevention. Appropriate signage has been installed in either the immediate or general vicinity of cameras to advise that cameras are in operation.

Security, Storage and Retention

The footage is stored securely and will only be viewed and accessed by authorised people. The footage is retained in accordance with the *Public Records Act 2002*, which in most cases is 30 – 90 days, unless it is required for official purposes, or as a public record.

Disclosure

Footage may be accessed by third parties in accordance with IPP11. Reasons for disclosing information include:

- for law enforcement purposes;
- for official investigations;
- where individuals have agreed to the disclosure of their information;
- where it is necessary for the health, safety or welfare of individuals or public health reasons; or
- when otherwise required by law, including under the *Right to Information Act 2009*.

Public request for access

You can apply to access your personal information, including surveillance camera footage, under the *Right to Information Act 2009* and *Information Privacy Act 2009*. Applications must be made to the Information Access and Amendment Unit of the department. Application forms can be downloaded from the department's website or by contacting the department's Information Access and Amendment Unit on 1800 809 078.

Complaints about the way surveillance camera footage is collected, stored, used or disclosed

If you believe the department has breached your privacy in relation to surveillance footage containing images of you, you may make a privacy complaint to the department. Your complaint will be investigated in accordance with the department's Complaints Management Policy. For further information on how to make a complaint please contact the department's Complaints and Review Unit: Phone: (07) 3224 7179, Fax: (07) 3225 1912, Email: complain@communities.qld.gov.au.

If the complaint is about a breach of privacy which occurred on or after 1 December 2009, and you are not satisfied with the department's response or the department has not responded within 45 business days of your complaint, you may refer your privacy complaint to the Office of the Information Commissioner (OIC). For more information, visit the OIC website at www.oic.qld.gov.au.

Further information

For further information on privacy contact the department's Information Privacy Unit, on 3224 2935 or refer to www.privacy.qld.gov.au.

May 2013

Great state. Great opportunity.

Queensland Government