Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Privacy compliance and camera surveillance

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

The *Information Privacy Act 2009* (Qld) (IP Act) requires agencies[1] to handle personal information in compliance with the Queensland Privacy Principles (QPPs). This includes personal information captured using camera, e.g., closed circuit television (CCTV) systems and body worn cameras.

1.1 When will a camera capture personal information?

Personal information is any information about an identified individual or an individual who is reasonably identifiable from the information.[2] This includes still images, video footage, and audio recordings (collectively referred to in this guideline as **recordings**) of an identifiable individual.

Most cameras used by agencies will capture pictures or videos of individuals and many record audio. If an individual can be identified from the recording, e.g. because it's clear enough they can be recognised or their identity is linked to that footage in some other way, the recording will be personal information.

2.0 When can cameras be used?

Under QPP 3, agencies can only collect personal information that is reasonably necessary for, or directly related to, one or more of the agency's functions or activities. There are additional limitations if the information is sensitive information.

[1] Agency includes a Minister, bound contracted service provider, or other entity subject to the privacy principles.
[2] Section 12 of the IP Act.

Before using the cameras, agencies should consider:

- Is there a clearly articulated business case for establishing or extending a camera surveillance system, i.e. what operational purpose do the cameras serve and is that purpose part of the agency's responsibilities?
- Will the cameras serve the purpose, e.g. if they are intended to detect and prosecute illegal dumping, will the type of camera, the quality of its recordings, and its location achieve that goal?
- Is there an alternative to using cameras? Would live monitoring of the cameras serve the purpose without recording what the cameras capture?
- Has a Privacy Impact Assessment been conducted?
- Is use of the cameras lawful and fair?
- Will the cameras record sensitive information?

Refer to ***QPP 3 – collection of solicited personal information*** for more information.

1.1 Sensitive information

Sensitive information is a specific kind of personal information, defined in schedule 5 of the IP Act. It includes health information and information about religious or philosophical beliefs.

Under QPP 3, sensitive information can only be collected:

- where the information is reasonably necessary for or directly related to one or more agency functions/activities; and
- With the consent of the individual to whom the sensitive information relates (unless an exception applies).

If camera surveillance will capture sensitive information, for example CCTV cameras in a hospital that could record audio and video of doctors discussing a patient, the agency will need to ensure the CCTV recording system satisfies the sensitive information collection requirements.

Refer to ***Key concepts – personal and sensitive information*** and ***QPP 3 – collection of solicited personal information*** for more information.

2.0 What to tell people about the cameras

QPP 5 requires agencies to take reasonable steps to inform individuals of a range of relevant matters specified in QPP 5.2 when they collect personal information.

For CCTV or other fixed surveillance, the best way to comply with QPP 5 is by placing a sign near the cameras' location. Detailed information about the QPP 5 matters can also be included on the agency's website and/or in its QPP 1 privacy policy. Depending on the location and purpose of the cameras, agencies may prefer to place minimal, simple information on the sign along with details of where people can find out more information.

For more information refer to ***QPP 5 – Informing people when collecting personal information*****.**

Agencies which use body worn cameras may need to consider the best way to comply with QPP 5, as signage will rarely be a suitable option. This could be, for example, a verbal statement by the officers wearing the cameras or a pre-printed pamphlet or card the officers can hand out.

There are exceptions in the IP Act for law enforcement agencies and activities, e.g. an agency conducting covert surveillance does not need to advise the surveilled individuals of the QPP 5 matters, but these agencies/activities are not automatically exempt from the QPP 5 requirements.

For more information refer to ***QPP 3 & 6 - Law enforcement agencies and activities***.

3.0 Securing camera recordings

QPP 11 requires agencies to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure. Security measures are not one size fits all and must be adapted to suit the nature and sensitivity of the recording and the method by which it is collected, e.g., recorded to the camera's hard drive or transmitted wirelessly to the agency.

Security measures could include:

- Access controls for monitoring rooms and data storage areas.
- Ensuring the public and unauthorised agency officers cannot see or access screens on which the recordings are displayed.
- Access and audit controls for viewing, accessing, or copying recordings.
- Encryption of wireless recordings in transit and encryption or access controls on portable recordings, e.g. on body worn camera hard drives.

Agencies should also establish polices about access to and management of recordings, including:

- limiting as-of-right access to officers who require it as part of their duties
- protocols for requesting access, including procedures for disclosing recordings, e.g., to a law enforcement agency under QPP 6
- audit protocols for monitoring and recording who accesses the recordings and when; and
- protocols for disposal of recordings in compliance with the relevant Retention and Disposal Schedule.

QPP 11.2 also obliges agencies to take reasonable steps to destroy or de-deidentify personal information, where the agency no longer needs the information and it is not contained in a public record or otherwise legally required to be retained. Agencies will need to bear this in mind, in developing appropriate disposal protocols.

4.0 Using and disclosing the recordings

Under QPP 6.1, agencies can use or disclose personal information for the purpose it was collected or for any of the secondary purposes set out in QPP 6.1(a) and 6.2.

The secondary purposes include consent, for law enforcement activities, to prevent a serious threat to an individual or the public, and where authorised by law or a court.

Any internal request to use recordings or external request to disclose recordings for a secondary purpose must comply with QPP 6.

Refer to ***Key privacy concepts – use and disclosure*** and the relevant ***QPP 6 – Use or disclosure*** for more information.

4.1 Regular requests for recordings

An agency which receives regular requests for camera recordings, e.g., from the Queensland Police Service, should establish a protocol or procedure for assessing and approving those requests. A request form, to be completed by the requesting entity, will help ensure a compliant and efficient process.

OIC has developed an **Information Request Form template** (under development) which agencies may find helpful.

4.2 Access to the recordings

People can apply to access recordings under the *Right to Information Act 2009* (Qld) (RTI Act) and parties to a court process or their lawyers can subpoena recordings.

Agencies must ensure they have the tools and resources necessary to deal with those requests.

Agencies should also consider developing an administrative access scheme which allows individuals to access recordings of themselves, or recordings that contain no personal information or other information of concern, without a formal process. Care must be taken to ensure other individual's personal information, or information that could be contrary to the public interest to release under the RTI Act, is not disclosed.

For more information, refer to ***Managing access to Digital Video Recordings***.

5.0 Outsourcing camera and recording management

If an agency wants to outsource management of its cameras and recordings to a non-government contractor, it must comply with chapter 2, part 3 of the IP Act. This chapter of the IP Act requires agencies to take reasonable steps to bind a contracted service provider to the privacy principles when the contract will involve personal information moving between the contractor and the agency.

Agencies should also consider their obligations under the RTI Act and ensure any outsourcing arrangement provides for the easy retrieval of recordings.

Additionally, agencies should ***also*** consider potential obligations under the Mandatory Notification of Data Breach scheme established by Chapter 3A of the IP Act. The MNDB scheme applies to personal information contained in a document 'held' by an agency.[3] This includes personal information under the agency's control,[4] and may extend to recorded footage stored or managed by a contracted service provider.

Refer to ***Binding contractors to the IP Act*** (guideline under development) for more information.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published October 2024 and Last Updated 30 September 2024

[3] Section 46 of the IP Act.
[4] Section 13 of the IP Act.