Office of the Information Commissioner
Queensland

Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Camera Surveillance and Privacy

Queensland government agency systems which involve the collection and storage, use or disclosure of personal information are subject to the privacy obligations in the *Information Privacy Act 2009* (Qld) (**IP Act**). These obligations do not prevent an agency using camera surveillance for legitimate business activities; they will, however, affect the policies and practices associated with how the camera surveillance system operates.

This guideline outlines the privacy impacts agencies[1] must consider when implementing or extending a camera surveillance system.[2] The checklist in Appendix A will help you assess your agency's camera surveillance system for privacy compliance. In this guideline 'camera surveillance' includes any equipment used to observe and record images of individuals, such as closed circuit television (**CCTV**), temporary or fixed cameras (such as automatic number plate recognition cameras), body-worn video and unmanned aerial vehicles[3].

Is camera surveillance footage personal information?

Personal information is any information or opinion, whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[4]

If the camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from the footage.

Quality is determined by factors including the image size and resolution, position of the person to the camera, and the degree to which the individual's face or other identifying characteristics are visible.

If the person in the footage is identifiable, the footage will reveal information about that individual, for example that they were present in that space at that time. As such, camera surveillance footage potentially contains personal information and the obligations in the privacy principles apply.

[1] In this Guideline references to an 'agency' include Ministers and bound contracted service providers, unless otherwise specified.
[2] See OIC's Guideline *Undertaking a Privacy Impact Assessment* for further detail on how to identify and address the privacy impacts of a new project.
[3] For more information on drones, please see OIC's guidelines on Privacy and Drone technology.
[4] Section 12 of the IP Act.

Is camera surveillance right for you?

An agency must not collect personal information unless the information is necessary to fulfil a purpose directly related to a function of the agency.[5] Before installing a camera surveillance system, you must determine what the proposed camera surveillance is intended to achieve and be able to clearly articulate the agency function or activity this relates to. Once the purpose is identified, you must consider whether camera surveillance is necessary to achieve this purpose.

Questions to consider

- Is there research available that supports the use of camera surveillance for your identified purpose?
- Have you considered whether there is an alternative strategy to achieve this purpose, or whether camera surveillance would be more effective as part of a suite of strategies, such as upgraded lighting?

Is the camera surveillance system fit for the purpose?

Agencies must ensure personal information they collect is relevant to the purpose for which it was collected and that the collection itself does not unreasonably intrude into the personal affairs of the individual.[6] This means you need to carefully consider the location and position of cameras—as well as the technical specifications of the equipment you choose—to ensure the cameras only collect necessary and relevant personal information in a way that does not unreasonably intrude into someone's personal affairs.

Example

Your agency has identified that camera surveillance is needed to deter property crime and assist in the investigation and prosecution of criminal offences. To ensure that the collection of personal information is necessary and relevant for this purpose, you may need to consider:

- Will the location of the camera only view areas that are relevant to the intended purpose?
- Will the proposed location unreasonably intrude on someone's personal affairs, for example, by capturing private property or the entrance to a doctor's office?
- What camera position or angle is necessary to capture relevant images?
- What image size, resolution and capture rate is necessary to enable identification of individuals?

[5] Information Privacy Principle (IPP) 1 and National Privacy Principle (NPP) 1.
[6] IPP 3 and NPP 1.

- How will footage be exported from the system to create a record for investigation or evidentiary purposes?

What do I have to tell people about the camera surveillance system?

You must take reasonable steps to make individuals aware of the purpose and legislative authority (if any) for collecting personal information and any entities to which the agency usually discloses information of that kind.[7]

An effective way of meeting this obligation is to place a prominent sign at the entrance to the camera surveillance system's area of operation and reinforce this with further signs near each camera. This allows people to know about the camera surveillance system before they are close enough to be captured and should prevent claims the surveillance is occurring unfairly. Signs should also identify which agency operates the cameras. Camera footage can be applied for under the *Right to Information Act* 2009 and Chapter 3 of the IP Act, but this right can only be exercised if it is clear which agency operates the cameras.

Example notice

Camera surveillance operates in this area to ensure public safety and for the investigation and prosecution of criminal offences. Footage will only be accessed by persons authorised to do so. Should an incident occur, footage may be provided to the Queensland Police Service for law enforcement purposes. Your information will not be given to any other person or agency unless authorised or required by law.

Enquiries may be directed to [Agency Name] by calling [agency number].

You should consider whether additional steps can be taken to make people aware of camera surveillance in use by your agency, such as:

- making your agency's policy and procedures governing the management of camera surveillance systems publicly available
- publishing a fact sheet about why camera surveillance is used and how your agency meets its obligations under the IP Act
- publicising the operation of 'safe-city monitoring', for example in an online interactive mapping tool[8]
- engaging with local residents and retailers about the location of proposed new cameras; and
- incorporating information about the use of camera surveillance into staff induction.

[7] IPP 2 and NPP 1.
[8] For example, City of Melbourne publish detailed information about their Safe City Camera Program, including camera location map and annual audit reports on the operations of the camera program, viewable at http://www.melbourne.vic.gov.au/COMMUNITYSERVICES/COMMUNITYSAFETY/Pages/SafeCitycameras.aspx.

Tip

Documented policies and procedures which address the privacy considerations of using camera surveillance will help ensure compliance with the requirements of the IP Act, clarify responsibilities, and ensure consistency in decision making and operational practices.

Agencies are required to provide information to the public about the personal information they hold, what it is used for, and how it can be accessed.[9] This is often done through a privacy plan or information digest located on an agency's website. It may be necessary to update your agency's personal information holdings to include camera surveillance footage.

How do I secure footage collected by camera surveillance?

Personal information must be adequately protected against misuse, loss, and unauthorised access, use and disclosure.[10] This means protecting both stored camera footage and areas where monitoring of camera surveillance takes place. Potential security measures include physical, technical and operational safeguards.

Physical safeguards include suitable housing for digital recorders, placing cameras out of reach, using locks and swipe cards for access to control rooms and data storage areas, positioning monitors or using barriers and screens so live footage cannot be viewed by unauthorised persons[11].

Technical safeguards include using password protection to manage staff access to stored footage, transmitting and storing footage in encrypted form, encrypting any footage stored on portable storage devices, and securely deleting or writing over footage you no longer need.

Operational safeguards involve establishing documented policies and practices about access to footage such as:

- limiting the number of staff who can access footage and/or control rooms to those who 'need to know' and having a standardised, auditable process for when access is granted
- maintaining an audit trail of who accesses footage and when it was accessed; and
- establishing clear protocols for responding to requests for access to, or copies of, footage (for example, who has authority to release footage and how copies of footage are to be transferred).

[9] IPP 5 and NPP 5.
[10] IPP 4 and NPP 4.
[11] Viewing of live images on monitors should usually be restricted to the operator and any other authorised person where it is necessary for them to see it, unless the monitor displays a scene which is also in plain sight from the monitor location. For example, customers in a bank can see themselves on a monitor screen. This is acceptable as they cannot see anything on the screen which they could not see by looking around them.

Whether a safeguard is adequate will depend on the type and amount of personal information being collected and the nature of the equipment. For example, body worn video cameras that attach to the outside of clothing may require additional controls such as password protection and encryption software to protect recorded footage from unauthorised access should the device be lost or stolen.

Hint

If you are using or intend to use a cloud-based service to store camera footage, you should consider whether the security measures of the cloud provider provide an adequate level of protection. If the cloud service provider's servers are located overseas, you will also need to consider section 33 of the IP Act, which set out the circumstances in which an agency may transfer personal information outside of Australia.

When can I delete the footage?

Keeping personal information for no longer than is necessary, and disposing of it appropriately, will help protect personal information from misuse, loss and unauthorised access, modification or disclosure.[12]

Camera surveillance footage created by agencies may be a public record. As such, you need to consider your agency's recordkeeping obligations under the *Public Records Act 2002* (Qld) and associated recordkeeping regulatory requirements. Footage that is a public record must be retained for at least the minimum retention period specified in the *General Retention and Disposal Schedule for Administrative Records* or an agency or sector specific Retention and Disposal Schedule that has been approved by the State Archivist.

Example

An extract or copy of camera surveillance footage is created as part of an investigation into a workplace accident. It is likely that the agency will need to manage the extracted or copied footage as a public record.

Queensland State Archives can give you more information about retention requirements that may affect camera surveillance footage.[13]

What can I use the footage for?

Under the IP Act, you can only use personal information for the purpose for which it was obtained, unless one of the exceptions applies.[14] These include using it with the individual's consent, under a legislative authority, for law enforcement purposes or to prevent risks to for health and safety.

[12] IPP 4 and NPP 4.
[13] https://www.forgov.qld.gov.au/surveillance-records
[14] IPP 10 and NPP 2.

If your agency is not a health agency, you can only use that part of the camera surveillance footage that is directly relevant to what you are trying to achieve[15]. For example, if you have multiple footage of an individual involved in a specific incident and the footage needs to be used by the agency, you must only use those portions of the footage surrounding, or relevant to, the incident.

When can I disclose footage?

The IP Act contains rules for when you can disclose[16] personal information to a third party.[17] This includes where the individual was reasonably made aware that this would occur (for example, there was a sign near the camera which said the disclosure would occur), where the individual consents, under a legislative authority, for law enforcement purpose or to prevent risks to health and safety. It can also be applied for under the *Right to Information Act 2009* or Chapter 3 of the IP Act.

Requests from QPS or other law enforcement agencies

The IP Act allows agencies to disclose personal information to law enforcement agencies, including the Queensland Police Service (**QPS**), if the personal information is 'reasonably necessary' for a law enforcement activity.[18] This includes personal information contained in surveillance footage.

Each request must be assessed on a case-by-case basis. Using a request form like the ones set out in Appendix B (for non health-agencies) or Appendix C (for health agencies) will help you gather and record the information needed to assess the request. If your agency regularly provides footage to another agency, such as QPS, consider developing an agreement, such as a Memorandum of Understanding, that sets out how both agencies will meet their privacy obligations.[19]

When footage is disclosed for law enforcement purposes, the IP Act requires that a record of the disclosure is *included with the footage*.[20] One way to meet this requirement is to keep a copy of the footage and include with it a record of the agency's compliance with the request.

Subpoena and other notices of the court

If your agency receives a subpoena or other court order to produce footage, the disclosure is authorised or required by law.[21] However, this only applies to the footage covered by the description in the subpoena.

[15] IPP 9; there is no equivalent to IPP 9 in the National Privacy Principles.
[16] Disclosure is defined in section 23(2) of the IP Act.
[17] IPP 11 and NPP 2.
[18] IPP11(1)(e) and NPP 2(1)(g).
[19] Agencies other than health agencies should also consider the requirements in IPP 4(1)(b) to take all reasonable steps to prevent unauthorised use or disclosure of a document containing personal information that is given to a person in connection with the provision of a service to the agency.
[20] IPP 11(2) and NPP 2(2).
[21] IPP 11(1)(d) and NPP 2(1)(f).

Formal access applications under the IP Act or RTI Act

If an individual requests access to camera surveillance footage, and the footage shows only that individual, you may be able to release the footage administratively.

If there are other identifiable people in the footage, or an organisation or company requests access to footage containing identifiable people, it may not be possible to release the information administratively unless the footage can be securely redacted to remove personal information. In these circumstances, a formal application under the IP Act or RTI Act will be required.

What if I want to outsource management of the camera surveillance system?

In some circumstances an agency must take all reasonable steps to bind a contracted service provider to comply with the privacy principles.[22] This will generally be required where:

- they deal with personal information for the agency
- personal information will travel from the contracted service provider to the agency; or
- they are providing services to a third party for the agency.

The *Contracted Service Provider checklist*[23] will help you decide whether you have to bind the contracted service provider to comply with the privacy principles. Once bound, the contracted service provider is responsible for any breach of the privacy obligations in the IP Act and an individual is able to make a privacy complaint against the contracted service provider.[24]

If the contracting agency does not take all reasonable steps to bind the contracted service provider, the contracting agency will be responsible for any breach of privacy arising from the actions of the contracted service provider.[25] For more information about the privacy considerations when outsourcing, please see *Agency Privacy Obligations When Entering into Contracts and other Agreements*.[26]

Are there special rules for law enforcement agencies and activities?

The IP Act contains exemptions from, and exceptions to, the rules for law enforcement agencies. Agencies, or activities of agencies, that fall within these

[22] Chapter 2, part 4 of the IP Act.
[23] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers/contracted-service-provider-checklist
[24] Section 36(3) and section164 of the IP Act.
[25] Section 37 of the IP Act states that if the contracting agency fails to take reasonable steps to bind the contracted service provider, the obligations that would have attached to them had they been properly bound, instead attach to the contracting agency.
[26] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers

exceptions and exemptions may be entitled to disregard some of the privacy principles when conducting camera surveillance. For example:

- Section 29: the Queensland Police Service, Crime and Corruption Commission, corrective services, and other law enforcement agencies do not have to consider some privacy principles in some circumstances for some of their functions.
- Schedule 1, Section 1(a): camera surveillance footage arising out of or connected to a controlled operation or activity under the *Police Powers and Responsibility Act 2000* or the *Crime and Corruption Act 2001* is not subject to the privacy principles.
- Schedule 1, Section 1(b): camera surveillance footage arising out of or connected to a covert undertaking of an operation, investigation, or function of a law enforcement agency is not subject to the privacy principles.

See *Privacy and Law Enforcement Agencies*[27] for more information.

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

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 22 May 2013 and Last Updated 12 July 2018

[27] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-law-enforcement-agencies

Appendix A

Checklist for camera surveillance systems

The following checklist is a summary of the privacy considerations outlined in OIC's Guideline *Camera surveillance and privacy*. You may wish to use this checklist to satisfy yourself that your agency's camera surveillance system meets the obligations in the *Information Privacy Act 2009* (Qld).

Is camera surveillance right for you?

Have you identified a clear purpose/s for using camera surveillance?	
Can you articulate how this purpose relates to a function or activity of your agency?	
Can you show how the use of camera surveillance will achieve the identified purpose?	
Have you considered whether there are other options that could achieve the identified purpose more effectively than camera surveillance, or that could be used alongside camera surveillance to make it more effective?	

Is the camera surveillance system fit for purpose?

Are the cameras located and positioned so that they only view areas relevant to the intended purpose?	
Are the cameras located and positioned in a way that will not intrude to an unreasonable extent on the privacy of individuals, for example, by avoiding private property or an entrance to a doctor's office?	
Are the cameras capable of capturing the required image size and quality necessary to achieve the intended purpose?	

What do I have to tell people about the camera surveillance system?

Is there prominent signage[28] that notifies individuals of the reason and legislative authority (as appropriate) for using camera surveillance, and any entities to which the agency usually discloses footage?	
Is it clear who owns and operates the camera surveillance system?	

[28] Please refer to the full Guideline for an example.

Can the community easily find out further information about how your agency handles personal information captured via camera surveillance including the potential to access footage?	
Has your agency's list of personal information holdings been updated to include camera surveillance footage?	

How do I secure footage collected by camera surveillance?

Are safeguards in place to protect control rooms or areas where monitoring of camera surveillance occurs?	
Is there a standardised auditable process for when access is granted to these areas?	
Are safeguards in place to protect stored footage?	
Is there a standardised auditable process for when access is granted to stored footage?	

What if I want to use a cloud-based service to store camera footage?

Have you checked whether the servers are located overseas (even where the provider is an Australian company)?	
If the servers are located overseas, have you checked which provisions in section 33 of the IP Act can be relied on to authorise the transfer of personal information outside Australia?	
Do the security measures applied by the cloud service provider provide an adequate level of protection?	

When can I delete the footage?

Is camera surveillance footage regularly overwritten or otherwise disposed of[29] when it is no longer required by your agency?[30]	
Is information on your agency's retention and disposal of camera surveillance footage communicated to the community?	

[29] Storage of unneeded camera footage creates a vulnerability for misuse, loss or unauthorised access, use, modification or disclosure.
[30] Having regard to the obligations in the relevant Retention and Disposal Schedule issued by the Queensland State Archives.

Does your agency have a process for ensuring compliance with IPP 10/NPP 2 when it wishes to use camera surveillance footage for a purpose other than that for which it was initially obtained?	

When can I disclose footage?

Does your agency have policies and procedures about when and under what conditions camera surveillance footage may be disclosed to third parties?	
Does your agency have policies and procedures for individuals to request access to camera surveillance footage that includes their images?	
Is information publicly available on how individuals can request access to camera footage?	
Are documented business processes in place which establish how your agency will satisfy itself that footage is 'reasonably necessary' for a law enforcement activity[31] and the steps that must be taken to make a record of this disclosure?	

What if I want to outsource management of the camera surveillance system?

Will the contracted service provider in any way deal with personal information for your agency, or involve an exchange of personal information between your agency and the contracted service provider? If yes, have you taken all reasonable steps to contractually bind the contracted service provider to compliance with the privacy principles?	

[31] Please refer to the full Guideline for an example of a form used to handle requests from the Queensland Police Service to access footage.