Office of the Information Commissioner
Queensland

Applying the legislation

GUIDELINE

Drones and the Privacy Principles

Drones[1] are playing an increasing role in government service delivery. Potential uses include law enforcement, emergency and disaster management, infrastructure inspections and environmental monitoring.

Queensland government agencies which capture video and audio recordings using a drone must ensure that their collection, storage, use and disclosure of the recording complies with the privacy obligations in the *Information Privacy Act 2009* (Qld) (**IP Act**).

Personal information

Not all information collected by a drone will qualify as personal information. Personal information is any information about an individual who is or can reasonably be identified.[2] If the information is not about a reasonably identifiable individual, it falls outside the definition of personal information and does not attract the protections afforded by the IP Act.

An individual's image or voice is unique to that particular individual. Whether a recording of an individual's image or voice could reasonably identify that individual will depend on the quality of the recording. 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 it is uncertain whether the recording will be of sufficient quality to identify an individual, agencies should err on the side of caution by treating the information as personal information and handling it in accordance with the privacy principles.

What an individual was doing, where they were at a particular time or what they said is clearly information about the individual as it reveals a fact or opinion about them. Even if the information is about something other than an individual – a piece of land, for example – it can still be about an individual if there is a sufficient connection between the fact or opinion and the individual to reveal something about the individual.[3]

[1] Drone is the common term for Unmanned Aerial Vehicles (UAV) or Remotely Piloted Aircraft Systems (RPAS). In the context of this guideline, drone refers to any remotely controlled or autonomous ground-based crafts, aircrafts or underwater crafts.
[2] See section 12 of the IP Act for the full definition.
[3] For a more detailed discussion on this issue, see *Mahoney and Ipswich City Council* (310275, 17 June 2011) at https://www.oic.qld.gov.au/decisions/mahoney-and-ipswich-city-council.

Example

Florin Shire Council uses drones to survey its population of rodents of unusual size (ROUS), an invasive animal under the *Fire Swamp Act 1987*. While the information collected is about ROUS, it is subsequently matched with Council's property records and used to identify individuals who are unlawfully keeping ROUS. Information that a resident has not complied with animal management legislation is the personal information of that individual.

Privacy by design

Building in privacy protections from the start is less expensive or time-consuming than trying to retrofit them later. Conducting a Privacy Impact Assessment (**PIA**) when planning or initiating a project allows you to identify how the project may impact an individual's privacy and how the agency can mitigate those impacts. The privacy impacts of using a drone include:

- secondary use: information collected for one purpose is then used for another purpose
- lack of transparency: individuals are not made aware that they are under surveillance and do not understand what the information will be used for.
- intrusiveness: depending on where surveillance activities take place and what they capture, practices may be considered unreasonably intrusive and disproportionate to the purpose they are trying to achieve; and
- over-collection: surveillance activities may generate and capture more information than is necessary.[4]

Tip

One of the steps in conducting a PIA is to identify and consult with stakeholders. Consultation is an opportunity to address community concerns and build trust by showing that the agency has designed the project with privacy in mind.

Please see OIC's guideline: Undertaking a Privacy Impact Assessment[5] for further information.

[4] 'Guidelines to surveillance and privacy in the Victorian public sector' issued May 2017 by the Commissioner for Privacy and Data Protection, Victoria.
[5] Accessible from https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process

Collection

When an agency collects personal information it must ensure that the collection is for a lawful purpose directly related to a function or activity of the agency and that the collection is necessary to achieve that purpose.[6] The means by which personal information is collected must also not be unfair or unlawful.

It is imperative that agencies have a clear and specific purpose for which they will use information collected by the drone. Unless an agency knows what it intends to do with the personal information it collects, it cannot readily assess or assert its necessity or articulate how it relates to the performance of one of its functions or activities.

Incidental collection

One of the consequences of using drones is that the surveillance can record information incidental to that necessary to fulfil the intended purpose. For example, if an agency were to use drones to survey local parks for noxious weeds, it could collect images of any individuals in the park at that time. Accordingly, it is important to have a clearly defined purpose for the surveillance and that this purpose is directly related to a function or activity of the agency.

Regardless that it was not the agency's intention to capture images beyond that required for the function or activity, once it is in the agency's possession, the privacy principles governing storage and security, use, disclosure and overseas transfer nonetheless will then apply to any personal information in these incidental images.

Regardless of how an agency obtains personal information – deliberately or unintentionally – the recording becomes a document of an agency to which individuals have a right to seek access.

Notwithstanding the fact that the agency did not actively set out to record incidental images, there are still steps agencies can take to minimise the potential for there to be unneeded imagery. Agencies should look at where and when the drones will be deployed. In the example of using drones to survey local parks for noxious weeds, an agency could minimise what personal information it collects by deploying the drone at a time when the park is least busy or avoiding more popular areas of the park such as a playground or off-leash dog area.

Providing good communication on the agency's use of drones in terms of time, date, area and intended purpose can assist in minimising the capture of incidental personal information.

[6] Information Privacy Principle (IPP) 1 for non-health agencies; National Privacy Principle (NPP) 1 for health agencies.

Lawful and fair collection

The way in which an agency collects personal information must be lawful and fair.[7]

In order for collection to be lawful, it must be done in accordance with the law. Agencies may need to seek legal advice on applicable laws when using a drone. For example, an agency may need to comply with:

- *Civil Aviation Safety Regulations 1988* (Cth) Part 101[8] in relation to aerial drones
- *Invasion of Privacy Act 1971* (Qld) in relation to audio recording of conversations
- The common law relating to trespass against a person
- section 227A of the *Criminal Code 1899* (Qld) concerning observations or recordings in circumstances where a reasonable adult would expect to afforded privacy
- Maritime Safety Queensland and Australian Maritime Safety Authority requirements for underwater drones; and/or
- *Major Events Act 2014* (Qld) in relation to operating an aircraft above a major event area.

Unreasonable intrusion

The way that an agency collects personal information must not be an unreasonable intrusion into an individual's personal affairs.[9] 'Personal affairs' references an individual's domestic environment as opposed to public or work areas.

Factors that may inform whether the collection of personal information is an unreasonable intrusion include:

- the type of place under observation
- the nature of the activity could be taking place
- whether there is a less privacy-invasive alternative available to achieve the intended purpose; and
- whether the use of drones is proportionate to the problem being addressed.

Making people aware of the collection

When an agency collects personal information from the individual it is about, it must take all reasonable steps to provide that individual with certain information.[10]

[7] IPP 1 and NPP 1.
[8] See https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia.
[9] IPP 3(b) and NPP 1(2).
[10] IPP 2 and NPP 1. NPP 1 also requires that health agencies take reasonable steps to ensure that the individual is or has been given a collection notice when information about the individual is collected is collected from someone else.

Sometimes referred to as a 'collection notice', this information must be provided at or before the time of collection or, if that is not practicable, as soon as practicable after.

A collection notice must make individuals aware of:

- why their personal information is being collected
- details of any law that allows or requires the collection; and
- any entity to whom it is the agency's *usual practice* to give the information.[11]

A common-sense practice[12] with collection notices about surveillance activities is to include information about an individual's right to seek access to the recordings and the process for requesting this access.

In some limited circumstances agencies are not required to provide a collection notice, for example, when delivering emergency[13] or health services[14] or where the agency is satisfied on reasonable grounds that noncompliance is necessary in order to achieve or carry out a law enforcement function[15].

A challenge when using drones is how to provide a collection notice when there is often no direct interaction with the individual concerned. A communication strategy may include:

- posting a news item or media release on the agency's website
- posting content on the agency's social media accounts
- placing physical signage around the area under surveillance
- distributing flyers to the letterboxes of affected households; and/or
- running a newspaper and/or radio advertisement; and/or
- putting up a banner at the 'launch site'.

What constitutes 'reasonable steps' will depend on factors such as the nature of the information being collected and how the agency will use and disclose the information.

[11] NPP1 also requires that the collection notice include the identity of the health agency and how to contact it, the fact that the individual is able to gain access to the information they have provided, and the main consequences, if any, for the individual if all or part of the information is not provided.
[12] Health agencies are required under NPP 1(3)(b) to take reasonable steps to ensure that the individual is aware of the fact that he or she is able to gain access to the information at or before the time or, if that is practicable, as soon as practicable after it collects personal information. Agencies other than health agencies have an obligation under IPP 5(1)(d) to take all reasonable steps to ensure that a person can find out what they should do to obtain access to an document containing their personal information.
[13] IPP 2(5).
[14] NPP 1(5).
[15] Section 29 of the IP Act. It is important to keep in mind that section 29 is not a 'blanket rule' or a rule that should be retrofitted; rather, it is determined on a case-by-case basis by considering the nature of the information being collected and the circumstances surrounding the collection.

Tip

A community engagement strategy can assist agencies to make well-informed decisions. It is a practical tool that assists in identifying affected stakeholders, what aspects can be influenced by stakeholders, and how the agency can best meet stakeholders' communication needs.

Security of personal information

Agencies are required to protect personal information from misuse, loss and unauthorised access, modification and disclosure.[16]

Drones collect information in one of two ways:

- recordings are stored on-board (for example, on a memory card or hard drive); or
- recordings are transmitted back to a central device where they are then stored.

Both methods have vulnerabilities. If a drone with on-board storage becomes lost or captured by an unauthorised third party, so too will any information it carries. If the drone transmits information through a wireless connection, this connection can be intercepted and used to access or modify the information in transmission. Adequate safeguards such as password protection and encryption should be utilised to address these vulnerabilities.

Other safeguards that should be considered include:

- limiting the staff who can access stored recordings to those who 'need to know'
- maintaining an audit log of who accesses stored recordings and when it was accessed; and
- establishing clear protocols for responding to requests for access to, or copies of, recordings (for example, who has authority to release recordings in response to a request from a law enforcement agency).

Personal information holdings

Agencies must take all reasonable steps to ensure that an individual can find out the type of personal information it holds and the main purposes for which this information is used.[17]

[16] IPP 4 and NPP 4.
[17] IPP 5 and NPP 5.

In addition:

- Agencies - other than health agencies - must include information on what an individual should do to obtain access to a document containing their personal information.
- Health agencies must include information on how they collect and disclose that information.

This enables the community to exercise their right of access to information held by government by making it easier for them to find out what personal information the agency might hold about them.

Agencies commonly meet this obligation by publishing a list of its personal information holdings on its website, most commonly in a 'privacy plan'. Agencies should ensure that this list is updated to include details of the personal information it collected by using drones.

For guidance on managing requests for access to drone recordings, please see OIC's Guideline: Managing access to Digital Video Recordings.[18]

Use and disclosure of personal information

Agencies can only use personal information for a purpose other than that for which it was collected[19] or disclose the personal information to a third party[20] if one of the permitted exceptions in the IP Act applies.[21]

Permitted exceptions include:

- where the individual is reasonably likely to have been made aware that the disclosure would occur [22]
- the individual it is about expressly or impliedly agreed to the use or disclosure
- the use or disclosure is reasonably necessary to lessen or prevent a serious risk to an individual or to the public
- the use or disclosure is authorised or required under a law
- the use or disclosure is reasonably necessary for a law enforcement activity[23]
- the use or disclosure is for a limited research purpose; or
- for health agencies only, the individual would reasonably expect the

[18] Accessible from https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/processing-applications/managing-access-to-digital-video-recordings
[19] IPP 10 and NPP 2.
[20] IPP 11 and NPP 2.
[21] Under NPP 2,a health agency can disclose an individual's personal information to a third party without relying on a permitted exception if the disclosure is for the purpose for which the information was obtained in the first place, ie the primary purpose. It is only when the disclosure is for a different purpose altogether – a secondary purpose – that one of the permitted exceptions in NPP 2 needs to be satisfied.
[22] If the agency can foresee that it will be their usual practice to pass any of the personal information collected by the drone to a third party, it should make this clear in the collection notice provided to the individual.
[23] 'Law enforcement activity' does not include all activities of a law enforcement agency. See IPP 11(1)(e) and NPP 2(1)(g).

secondary use or disclosure, and it is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose.

Hint

Clear policies and procedures for the operation of an agency's drone program will help ensure that staff are aware of their obligations and understand how information collected by the drone can be handled. These policies and procedures should include:

- the purpose of the drone program
- what information is collected
- how information will be stored and how long information will be retained
- how requests to disclose or use information for another purpose will be managed
- who is permitted to access the information; and
- who the appropriate contact is within the agency, should staff or members of the public have questions about the program.

Outsourcing

If an agency will contract a third party to operate the drone or to outsource its management of information collected by the drone, it must take all reasonable steps to ensure that the contracted service provider is contractually bound to comply with the privacy principles.[24]

Once bound, the contracted service provider is responsible for any privacy breaches. 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.

For more information about the privacy considerations when outsourcing, please see OIC's guidance on the privacy considerations when entering into a service arrangement.[25]

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.

[24] Chapter 2, part 4 of the IP Act.
[25] Accessible at https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers/overview-of-agency-privacy-obligations-when-entering-into-contracts-and-other-agreements/part-two.

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 16 April 2018 and Last Updated 16 April 2018

Changes to legislation after the update date are not included in this document