Use of Drones - Guidelines for Municipal Police Services

These guidelines provide considerations for municipal police services when using drone technology.

October 2023

Office of the
Saskatchewan Information
and Privacy Commissioner

Use of Drones - Guidelines for Municipal Police Services

Introduction

Drones, an aircraft without a pilot (sometimes called an unmanned aerial vehicle (UAV)), are a technology launched into the air that can be used for a variety of purposes. Police services in Canada already use drones to assist in their work. Since drones can potentially be used to conduct surveillance, many privacy concerns exist regarding their use.

Municipal police services in Saskatchewan are subject to *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). This resource is meant to provide guidance to police services on their use of drone technology.

I. Before Implementing the Use of Drones

Some considerations for a police service before implementing the use of drones is to determine:

- Is the use of drones lawful.
- Is the use of drones necessary.
- Are there any stakeholders that should be consulted.

Is the Use of Drones Lawful

As local authorities, municipal police services must only collect personal information in accordance with section 24 of LA FOIP. Section 24 of LA FOIP provides:

> **24** No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

Municipal police services cannot collect personal information for an undefined purpose. Municipal police services must determine if the purpose for collecting personal information via drone technology relates to an existing proposed program or activity of the local authority.

If so, municipal police services must also ensure it has authority pursuant to sections 27 and 28 of LA FOIP to use and/or disclose any personal information it has collected.

Is the Use of Drones Necessary

Before using drone technology, municipal police services should consider if there are other less privacy invasive options to achieve the same goal. This may include using a more conventional camera to precisely capture images rather than a drone that may over-collect personal information.

Before using drone technology, the municipal police service should undertake a privacy impact assessment (PIA). A PIA will ensure that the municipal police service is considering requirements under LA FOIP such as authority for the collection, use, and/or disclosure of personal information, the storage and safeguarding of personal information and the retention and destruction of personal information. Municipal police services must also be cognizant that LA FOIP will provide individuals with right to access footage recorded by drone technology. Municipal police services will need to consider how it will be able to facilitate such access.

For more information about PIAs, check our PIA resources here: https://oipc.sk.ca/resources/resource-directory/privacy-impact-assessment-guidance-and-supporting-documentation/.

Are There any Stakeholders That Should be Consulted

Given how intrusive drone technology can be, municipal police services should determine if it should consult with relevant stakeholders and representatives of those potentially impacted. For example, if a municipal police service intends to use a drone in a particular neighbourhood for a period of time, then municipal police services should notify those who live and/or work in the area. This provides the municipal police services with the opportunity to communicate the purpose(s) of using drone technology. This would also be an opportunity for municipal police services to learn about specific privacy concerns and address them. This may also be an opportunity for municipal police services to consider privacy risks they did not previously identify and to explore options to mitigate such risks.

II. Once the Decision to Implement Drone Technology is Made

Below are some considerations for the municipal police service once it has decided it will use drone technology:

- Is the duty to protect being met.

- What measures can be taken to minimize the impact to personal privacy.
- What safeguards should be put in place to properly protect the personal information.
- How will access to information requests for video surveillance footage be handled.

Is the Duty to Protect being Met

Section 23.1 of LA FOIP requires that a local authority have administrative, technical and physical safeguards to protect personal information.

Administrative safeguards are controls such as written policies and procedures regarding how personal information is to be managed and protected. In the case of drone footage, examples of administrative safeguards may include where the footage is saved and who can access it and for what purpose, how long the footage is to be retained and when it can be destroyed. Administrative safeguards also include agreements with information management service providers (IMSPs) that manage the footage on behalf of the police service, and audits to ensure the footage is being accessed only on a need-to-know basis.

Technical safeguards mean the technology and the policy and procedures that are used to protect personal information and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

Physical safeguards are physical measures to protect personal information. They include protecting buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems and clean desk approaches.

What Measures can be Taken to Minimize the Impact to Personal Privacy

Collection occurs when an individual's image is captured by the video surveillance system. Municipal police services who are implementing the use of video surveillance will need to ensure they have proper authority under LA FOIP for collecting the personal information of individuals. Some things public bodies should consider:

- In what circumstances and for what purposes will drone technology be used.
- Is it possible to use the drone in a way to minimize the likelihood of capturing personal information.

- Will the public/impacted individuals be notified of the drone being used pursuant to section 25 of LA FOIP.
- How will the municipal police service handle the potential over-collection of personal information.

What Safeguards Should be put in Place to Properly Protect the Personal Information

Once municipal police services have collected personal information, they will need to ensure that they are storing the information in a proper manner and have sufficient safeguards to protect it from improper use or disclosure.

- Ensure proper policies are in place for the collection, use, disclosure, destruction and access to information of footage.
- Ensure proper technical safeguards are in place to adequately protect personal information collected by the drone.
- Provide training for employees who will have access to drone footage.
- Determine the frequency of audits and what the audit will look for (such as user accesses).
- Need-to-know – limit the number of employees that can access the drone footage to those that have a legitimate need-to-know.

How Will Access to Information Requests for Video Surveillance Footage be Handled

Once collected, an individual's personal information as recorded by a drone becomes a record that individuals could request access to. Just as with other records, public bodies will need to determine how they will provide individuals with their right to access this information while protecting the personal information (or images) of other individuals captured by the drone. Software that allows the ability to blur out images may be an option that municipal police services want to acquire.

III. After Implementing the use of Drone Technology

A consideration for the municipal police service after implementing the use of drone technology is to evaluate and audit its use.

Evaluation and Audit of Drone Technology

Once a municipal police service has implemented the use of drone technology, it will need to regularly conduct audits to ensure employees are following policies and procedures. The audit should reveal any issues with compliance. For example, it may reveal an employee is accessing the footage, but they do not have a professional "need-to-know" for viewing it. The municipal police should address the issues in a timely fashion to maintain the confidentiality and integrity of the record.

As well, the municipal police service should regularly evaluate if the use of drone technology is a necessary practice. The evaluation could consider the frequency in which it uses drone technology, for what purposes and the effectiveness of using drone technology to achieve the purposes.

IPC Consultation Process

Our office will provide feedback on a PIA or drafted policies and procedures as part of a consultation process. If you are considering using drone technology, you can submit your PIA and/or drafted policies to our office for consultation. While our office prefers that we are provided the opportunity to provide consultative advice prior to the implementation of a program or practice, our office may provide comments on programs or practices already in place. For more information on the consultation process, please see under the *For Public Bodies* tab: https://oipc.sk.ca/assets/consultation-request-form.pdf

Contact Information

If you have any questions or concerns about these guidelines or if you would like to request an investigation or review involving video surveillance, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC