



Office of the
Privacy Commissioner
of Canada

Drones in Canada

Will the proliferation of domestic drone use in
Canada raise new concerns for privacy?

*Report prepared by the Research Group of the
Office of the Privacy Commission of Canada*

March 2013

Table of Contents

INTRODUCTION.....	1
PART ONE: DRONE 101	2
Drone Terminology: What is a drone?.....	2
Drone Types: What do drones look like?.....	3
Drone Attributes: What can drones do?.....	3
PART TWO: DRONE APPLICATIONS.....	4
a) Private Sector.....	5
b) Public Sector	5
c) Recreational.....	5
PART THREE: DRONE REGULATION	6
What are the Current Roles in Canada Governing Drones?	6
Safety Still the Primary Concern of Aviation Regulators	7
PART FOUR: PRIVACY CONSIDERATIONS.....	10
Privacy Implications	10
a) The changing nature of surveillance.....	10
b) Expectations of Privacy in Public	12
Drones and Canadian Privacy Laws and Guidance	13
CONCLUSION: WHAT WILL HAPPEN NEXT?	14

INTRODUCTION

Drones are remarkable devices. They can hover in midair, do back flips and spins; they can maneuver smoothly and precisely through small spaces or in concert with other drones; and they can do all this while carrying things like a stabilized video camera and a multitude of other technologies on board. The extent of their versatility is what makes them a viable option for a number of different tasks. Drones can be deployed as weapons in far-away wars, or can help reinvent the way humanitarian aid is provided.¹ Drones can help advance scientific research, or can perform tracking and monitoring and surveillance work. Drones could revolutionize the way humans do certain work or even perform dangerous tasks, but they could also encroach on the core values of a free and democratic society. Drones have unique capabilities and are very flexible in terms of the tasks they can perform, which is what is making them a desirable alternative to manned flights.

Drones are no longer exclusively for military use on the battlefield. They have been evolving into a more accessible tool that could eventually be put to various tasks domestically across North America. Drones do currently operate in limited circumstances in Canada, and their use is steadily on the rise. In addition to their projected proliferation in the public and private sectors here at home, they are also increasingly becoming available to Canadian citizens at large.



Drone technology raises important questions and concerns about privacy. There is a gap in regulation, which does not address issues related to purpose and the privacy implications of their use. Current regulations governing drone operations have more to do with ensuring their safe flight, and do little to address the privacy implications of having Canadian skies filled with hovering data-collecting robots.

The purpose of this research report is to explore the emergence and privacy impacts of drone technology in Canada, and question how the proliferation of their use in Canada could present new concerns from a privacy perspective. Part 1 of this report provides an overview of drone terminology, drone types and drone attributes. Part 2 sets out to explore some of the current and prospective uses for drones in a domestic context, covering the public and private sectors and also recreational use. Part 3 will set out the current state of affairs in Canada in terms of regulating drone flight, and outline how outstanding safety concerns remain the primary barrier to their implementation in certain contexts, with only few codes of conduct making mention of privacy as a concern related to drone flights. Part 4 examines how the unique characteristics of drones could have distinct privacy implications, and how Canada's privacy laws and existing guidance would likely apply to the use of drones.

PART ONE: DRONE 101

Drone Terminology: What is a drone?

Many people generally understand the term “drone” to describe an aircraft without an on-board pilot, or unmanned aircraft. In effect, the term “drone” is a catch-all term that refers to any vehicle that can operate on surfaces or in the air without a person on board to control it; and that can vary in size, shape, form, speed, and a whole host of other attributes.² A drone can be a model aircraft someone purchases in a store, a mini-helicopter used by some police forces, or a large plane-sized aircraft sent to a war zone.

In the industry, and across different regions, drones are also called Unmanned Air Vehicle (UAV), Unmanned Air System (UAS) or Remote Piloted Aircraft Systems (RPAS). The International Civil Aviation Organization (ICAO) has set a new definition referring to drones as RPAS, which will soon become the recommended term internationally as ICAO moves towards developing standards for member states. The following are definitions associated with the various drone terminology:

- **UAVs** (Unmanned Air Vehicle) UAV is a “power driven aircraft, other than a model aircraft, that is designed to fly without a human operator on board.”³
- **UAS** (Unmanned Air Systems) – A UAS is an unmanned aircraft (UA) and all of the associated support equipment, control station, data links, telemetry, communications and navigation equipment, etc., necessary to operate the unmanned aircraft.⁴
- **RPAS** (Remote Piloted Aircraft Systems) – A newly emerging definition coming from the International Civil Aviation Organization that intends to highlight the fact that the systems involved are not fully automatic but always have a pilot in command responsible for the flight.⁵ RPAS describes a remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components as specified in the design.⁶
- **Model Aircraft** is an aircraft, the total weight of which does not exceed 35kg (77.2 pounds) that is mechanically driven or launched into flight for recreational purposes and that is not designed to carry persons or other living creatures.⁷

While there are some slight differences in their definition, UAV, UAS and RPAS can essentially be used interchangeably to refer to unmanned aircraft and the systems that connect them to their pilots on the ground. Model aircraft on the other hand, are distinctly different from UAVs in the fact that they are used for purely recreational purposes, and thus not covered by regulation. This paper will use the terms UAVs, UAS and RPAS interchangeably or refer to them commonly as “drones.”

Drone Types: What do drones look like?

Drones can range in size and form and are typically described according to weight, endurance, purpose of use, and altitude of operation.⁸ Some look like mini-airplanes with fixed-wings, others are like mini-helicopters, and some even look like birds or other animals. They can be as large as traditional manned aircraft, or small enough to fit in a backpack. Large drones can fly at high altitudes and some can even remain airborne for several days.

The aircraft themselves are steadily improving, becoming smaller, cheaper and smarter. Small drones costing \$30,000 to \$50,000 are almost equivalent to the cost of a police cruiser, and much less expensive than a manned helicopter.⁹ Some drones are so small and quiet they could be undetectable to a person being surveilled.¹⁰ While there are a multitude of different types of drones, the following categories provide a helpful description of some of the different forms they can take.¹¹

- **Large fixed-wing aircraft:** Such as the Predator ([see photo](#)) or the Global Hawk ([see photo](#)). The Predator was the first-ever weaponized UAV, and has been used to gather intelligence and carry out targeted strikes in overseas operations. It can fly up to 25,000 feet for up to 40 hours.¹² More recently, the Predator has been adapted for surveillance missions on the U.S. borders, including the U.S.-Canada border.¹³ Unlike the Predator, the Global Hawk is used primarily for surveillance and is not armed.¹⁴ It is capable of staying aloft for up to 35 hours, transmitting video to ground stations during its flight. It is also used by NASA as a “Hurricane Hunter.”¹⁵ The T-Hawk has the capacity to hover and stare, inspect from close range and pursue a target.¹⁶ These types of large fixed-wing drones are the most similar to manned aircraft. Their size and range of flight enables these UAVs to be configured with a range of different payloads capable of persistent and highly sophisticated surveillance.
- **Small fixed-wing aircraft:** Aircraft such as the Boeing ScanEagle ([see photo](#)) can stay aloft for more than 24 hours and can fly at 19,500 feet. These types of aircraft are becoming more popular domestically in the U.S. for use by local law enforcement.¹⁷
- **Micro-UAVs:** Sometimes referred to as “Backpack craft” or “mini-helicopters”, they are cheap and portable, designed to be carried and operated by a single person. While their price range makes them within reach for hobbyists, they are also often popular for law enforcement operations. Some examples are the \$300 Parrot AR Drone¹⁸ or the DraganFlyer X6 used by the RCMP ([see photo](#)).
- **Biomimetic UAVs:**¹⁹ Drones that imitate naturally-occurring animals or plants (commonly birds, snakes and insects), such as AeroVironment’s Nano Hummingbird ([see photo](#)).
- **Blimps or balloons:** Although not commonly thought of as drones, unmanned blimps or balloons can sit up in the sky in one place, observing for long periods of time.²⁰ These types of UAVs are currently being tested along the U.S. – Mexico border ([see photo](#)).²¹

Drone Attributes: What can drones do?

Drones are often referred to as a desirable alternative to manned flights, and it is largely due to their flexibility and unique capabilities. Drones can be a persistent, highly targeted and cheap form of surveillance. Drones can be deployed on demand and can generally stay in the air longer than manned aircraft. They are flexible in terms of the tasks they can perform, they can support high-resolution imagery and sensors, and the “plug and

play” payload capability makes them easy to tailor to a specific flight purpose. Furthermore, they can cover vast and remote areas.²² Some of the advanced surveillance technologies that can be mounted on drones include:²³

- **High-power zoom lenses** that could increase the chances of individuals being surveilled from a great distance.
- **Night vision, infrared, ultraviolet, thermal imaging, and LIDAR (light detection and ranging)** that enables UAVs to detect and enhance detail.
- **Radar technologies** that can penetrate walls and earth enabling the tracking of individuals even inside buildings, through cloudy conditions and through foliage.
- **Video analytics technology**, which is improving rapidly and would be able to recognize and respond to specific people, events and objects, or even flag changes in routines to identify particular movement patterns as “suspicious”. This could also include things like license plate readers.
- **Distributed video**, whereby a number of UAVs work in concert with multiple video cameras.
- **Facial recognition or other “soft biometric recognition”** that enables the UAV to recognize and track personal attributes such as height, age, gender and skin colour.

PART TWO: DRONE APPLICATIONS

Drones are often associated with their military purposes in the context of war abroad. However their use is beginning to expand beyond the original military applications into areas of civil aviation. The current and the speculated uses for drones range quite broadly across the public and private sectors. Government organizations, private sector entities and amateur enthusiasts are all seemingly eager to launch drones in domestic skies for a variety of purposes.

Currently in Canada, domestic UAV operations are extremely limited because they are subject to licensing approvals and safety parameters set by Transport Canada (see Part III of this paper). This limiting factor, however, “is not technological, but regulatory.”²⁴ While the use of drones in Canada is still fairly limited by these regulatory and licensing parameters, Transport Canada has indicated on its website that UAVs “operate in diverse environments and in high risk roles, including but not limited to: atmospheric research (including weather and atmospheric gas sampling), scientific research, oceanographic research, geophysical research, mineral exploration, imaging spectrometry, telecommunications relay platforms, **police surveillance**, border patrol and reconnaissance, survey and inspection of remote power lines and pipelines, **traffic and accident surveillance**, emergency and disaster monitoring, cartography and mapping, search and rescue, agricultural spraying, aerial photography, promotion and advertising, weather reconnaissance, flight research, and fire fighting monitoring and management.”²⁵ **[emphasis added]**

Proponents of drones will often draw attention to the benign aspects of drones, such as describing them as no different from manned aircraft, or by focusing attention to the benefits, particularly for research and science such as tracking and predicting weather patterns.²⁶ However, much of the current policy debates surround the use of drones for certain types of monitoring and surveillance, particularly by law enforcement and for border patrol. While surveillance may be the most controversial use for drones, their features make them appealing for a wide variety of uses in both the public and private sectors.²⁷

Industry Canada expects that domestic applications within Canada will grow as Canadian Aviation Regulations incorporate UAVs and the industry becomes more commercially viable.²⁸ Moreover, it has been reported that worldwide markets are projected to double in the next ten years.²⁹ With this projected growth of the industry

and efforts to establish a regulatory framework UAVs will likely become a more common tool for civilian purposes in the very near future.

The technology is already here. Researchers are interested in them, government organizations are interested in them, and they are also available to the public. Anyone with a smartphone can easily own and operate a small camera-carrying drone for under \$350.³⁰ Drones are available for use by the public and private sectors, and for recreational use, so long as they are flown within the current regulatory parameters. The following sections contain some of the most commonly cited uses that are either occurring, or being contemplated in the public sector, private sector or recreational use.

a) Private Sector

In the private sector, drones are for the moment fairly restricted, but may increasingly become a practical tool for commercial businesses. It has been speculated that they could be utilized for profitable commercial services such as infrastructure inspection, communications and broadcast services, wireless communication relay and satellite augmentation systems, natural resources monitoring, media/entertainment, digital mapping, land and wildlife management, and air quality management/control.³¹ It is not far-fetched to imagine that drones could be used for aerial mapping services;³² the television and film industries could use drones to shoot advertisements and movies; or they could be used by real-estate agents to sell property.³³ It has also been suggested that drones could serve more off-putting purposes such as for paparazzi photographers or industrial espionage.³⁴ The list of potential purposes in the private sector is seemingly expanding at the same rate as the accessibility of the tool.

b) Public Sector

As for the public sector, in the near term law enforcement represents the greatest potential users of small drones domestically because they offer a simple and cost effective alternative to airborne law enforcement activities.³⁵ Police forces in the U.S., the UK and in Canada have reportedly used drones for certain law enforcement activities. In Canada this includes the RCMP and some provincial police forces.³⁶ According to current media reports, the RCMP and some provincial police forces use drones only for specific purposes such as to take aerial photos and videos at traffic collisions or crime scenes and in search-and-rescue operations. As per these reports, when the OPP launches their UAVs, they do so under very strict conditions, mainly for photographing crime scenes: they can go no higher than 120 meters, must stay within the operator's line of sight and cannot fly over people not involved in incidents.³⁷

Other public sector uses might emerge with the proliferation of drones in domestic skies. Given the features of the technology, one could imagine that other Government of Canada departments and agencies might also be interested in the use of UAVs for a variety of purposes, in areas such as national security intelligence gathering, critical infrastructure protection, public safety and crisis management, or in environmental research. The Canadian Forces continue to conduct testing for future surveillance missions in Canada's north through its annual sovereignty operation in the arctic, called operation NANOOK. Operation NANOOK has been conducted annually since 2007 and in its most recent operations has included testing UAVs on a number of tasks related to "territorial oversight and overview."³⁸ The purpose is to ensure there is domestic capability for the Canadian Forces UAV program in the future.³⁹

c) Recreational

Another emerging issue is the operation of model aircraft, which describes the operation of small drones flown solely for hobby or recreation. Model aircraft can be virtually indistinguishable from other small UAVs,

in fact, “the majority of pilotless planes that civilian agencies have their eyes on are little bigger than model aircraft and weigh much the same.”⁴⁰ While aviation authorities such as the FAA and Transport Canada are focused on developing rules for the operation of small drones, model aircraft may actually be left entirely unregulated despite the fact they can often operate in much the same way as UAVs operating for commercial or other purposes such as surveillance.

The operation of recreational drones or model aircraft present unique concerns given their reduced costs and increased capabilities, and that they do not require a license to operate. Drones are already being sold as toys in many retail stores.⁴¹ The next generation of recreational drones could prove to be even smaller and cheaper than the ones that currently exist. Based in the U.S., a company called Always Innovating has unveiled a new palm-sized drone design that would follow an individual and stream live video to their Smartphone.⁴² The “MeCam flying copter camera”, expected to arrive in stores in 2014, would cost a mere \$49 and come equipped with video recording and streaming capabilities so footage can easily be shared with other social media outlets.⁴³

PART THREE: DRONE REGULATION

What are the Current Roles in Canada Governing Drones?

At present, UAVs are regulated in Canada under two different licensing streams: Transport Canada is the civil regulatory authority and the Department of National Defence (DND) is the military authority.

Transport Canada is responsible for establishing, managing, and developing safety and security standards and regulations for civil aviation in Canada, and includes unmanned civil aviation. Civil operations include law enforcement, scientific research, or use by private sector companies for commercial purposes. Domestic or foreign military UAVs come under the authority of DND when operating in civil airspace or military restricted airspace. The focus of this paper is on the use of drones covered by civil aviation regulations.

UAV operations for civil or commercial purposes are only authorized to fly with a Special Flight Operations Certificate (SFOC) issued by Transport Canada. The *Canadian Aviation Regulations* (CARs) govern civil aviation safety and security in Canada, and by extension govern operation of UAVs in Canada to an equivalent level of safety as manned aircraft. According to section 602.41 of the CARs,⁴⁴ “no person shall operate an unmanned air vehicle in flight except in accordance with a Special Flight Operations Certificate (SFOC), or an air operator certificate.”⁴⁵

As the name implies, SFOCs are intended to be an authorization for flight under special cases that are specific to a geographical area and for a specific mission. An SFOC may be issued to authorize a UAV to operate for any civil purpose, including for surveillance. The information that must be contained in an application for an SFOC includes details such as: type and purpose of the operation; description of the aircraft; dates and times of the proposed flight; security plans and emergency contingency plans; and a detailed plan describing how the operation will be carried out including: altitude and routes where the operation will be carried out, the location of any obstacles, and the exact boundaries of the area for the operation.⁴⁶

SFOCs are generally short-term authorizations intended to be issued on a case-by-case basis. However long-term or blanket authorities can be granted in certain circumstances where the SFOCs are being issued to organizations with an established history of previously approved SFOCs. The blanket SFOC approvals may be permitted for a specific geographical area, or for a defined time period, for example up to a year, if the site

and mission requirements are identical for each flight. This is generally how SFOCs are granted to law enforcement, who would utilize the UAV on an on-demand basis (e.g. for crime scenes that are sectioned off or traffic accidents).

Prior to being granted an SFOC, the operator must be able to demonstrate that they are adequately equipped to safely operate the UAV in the desired environment, which includes managing any risks associated with operation of the UAV and ensuring the protection of other airspace users and the safety of persons and property on the ground. In a majority of cases SFOCs apply to UAV flights within visual line of sight, which means that the pilot or observer must be able to stay within visual contact of the aircraft. There is no defined visual range because the requirement is dependent on environmental factors, weather conditions or other objects such as trees or buildings that could obstruct view of the aircraft.

There are restrictions on the use of UAVs over urban areas.⁴⁷ Certain key conditions apply to all operations under an SFOC, one of which requires that the operator only fly the UAV “over areas that would permit a safe landing on the surface without hazard to persons or property in the event of any emergency requiring immediate descent.”⁴⁸ There can also be additional conditions that may not apply to all operations, but can be attached to an SFOC authorization, such as:⁴⁹

- the UAV shall not be operated over or within a built-up area of a city or town;
- the UAV shall not be operated within a certain distance of any built-up area of a city or town; or
- the UAV shall not be operated near noise sensitive areas, such as churches, hospitals, parks and schools.

The type of payload mounted on a UAV is only a consideration where there are safety concerns, for example, if the payload is an object that might interfere with the pilot’s ability to operate the aircraft. Payloads that may impact on privacy, such as a camera or other sensors, would not necessarily pose any limitations for issuing a SFOC.

The SFOCs are issued regionally by inspectors in Regional Transport Canada General Aviation Offices who review the merits of each application individually and assess safety concerns or risks associated with the proposed flight mission. Currently in Canada there are no established standards to set requirements for pilot licensing, certification, maintenance, or command and control of UAVs. Safe flight is Transport Canada’s primary concern when issuing the SFOC and privacy considerations are notably absent in the licensing requirements or regulations established by Transport Canada. At present, there are approximately 300 individually licensed UAV operators in Canada.

Model aircraft are largely excluded from regulation by Transport Canada, although the CARs make important distinctions between UAVs and model aircraft. According to the CARs, model aircraft do not exceed 35kgs in weight and are only operated for recreational purposes. However, once a model aircraft is launched for any reason other than recreational purposes, it is considered a UAV for the purposes of the CARs and can only operate with the authorization of a SFOC. (Additionally, aircraft that exceed 35kgs, even when used recreationally, can only be operated with the license authority of a SFOC.) The recreational purpose is the key distinguishing feature between a model aircraft and a UAV.

Safety Still the Primary Concern of Aviation Regulators

In the short term, the use of drones in Canada is fairly limited by safety concerns that prevent drones from operating in certain circumstances, and also by virtue of having to obtain an SFOC which is intended to be issued on a special case basis and is constrained to a geographic and time limitation. However, there has been

a great deal of global movement to address safety concerns and ultimately expand the regulatory parameters around the use of UAVs in domestic contexts. These global developments will undoubtedly play an influential role on the future regulation of drones in the Canadian context.

Early in 2012, President Obama signed the “*FAA Modernization and Reform Act of 2012*”, which will provide funding to the Federal Aviation Authority (FAA) over the next four years to establish safety rules that will accelerate the integration and broad civilian use of unmanned aircraft in U.S. airspace by 2015. The key sections direct the implementation of draft plans, standards, and rules to ensure that drone integration proceeds in a safe and legal manner.⁵⁰ Set in motion by \$63 billion in funding and the relaxing of restrictions, the FAA is estimating that 30,000 drones will be approved to fly in U.S. skies in the next 20 years, up from the current 300 authorization certificates that have been issued to date.

The European Union (EU) has also been exploring the use of UAVs or drones for military and law enforcement applications. The FAA has established agreements with the EU to “initiate, coordinate, and prioritize the activities to support the development of provisions that would give UAVs full recognition as a legitimate airspace user.”⁵¹ In the context of the Europe 2020 Strategy,⁵² the emerging technology in the area of remotely piloted aircraft and the prospects for civil applications by commercial, corporate or government entities are being viewed as a source of economic growth and industrial competitiveness.⁵³ By the end of 2012, the European RPAS Steering Group (ERSG) promised to develop a comprehensive roadmap defining milestones and timeframes for the integration of civil RPAS in the European airspace, and will subsequently monitor the roadmap’s implementation.⁵⁴

In keeping with global developments, the ultimate goal for Transport Canada is to “normalize” UAV operations within civil airspace. Currently, the statutory framework that regulates UAVs in Canada is largely not UAV-specific and does not expressly permit routine UAV operations, nor does it govern the operation of UAVs in terms of their functions and purposes or effects. Moreover, the current decentralized and ad-hoc manner in which SFOC authorizations are issued makes it difficult for the public to know who has obtained an authorization to operate a UAV at any given time or for what purpose.

Since 2010, the Canadian Aviation Regulation Advisory Council (CARAC) Unmanned Air Vehicle (UAV) Systems Program Design Working Group has been working towards making recommendations for amendments or to introduce new regulations and standards that would facilitate the safe integration of routine UAV operations in Canadian airspace. Additionally, the Regulatory Cooperation Council (RCC), a U.S.-Canada Working Group, was established to harmonize regulatory approaches between the two countries in trade, travel and security. One aspect of the RCC working group is to formalize discussions and work towards aligning approaches and harmonizing regulations around UAVs in Canada and the U.S. where feasible.⁵⁵ It is unclear at this time how those efforts and any future regulatory changes will affect the approach taken in Canada with respect to the use of UAVs, or how closely they will emulate the developments in the U.S.

The current push to expand regulations around the use of drones for civil purposes is largely focused on the safety aspects of their flight, particularly if they are to operate beyond line of sight and in populated urban areas here at home. This focus is clear when we look at the objectives of the FAA in the U.S. or Transport Canada with respect to UAVs; both of which are concerned primarily with safety of flight while permitting, to the greatest extent possible, routine UAV operations.⁵⁶

Beyond this, aviation regulators believe they do not have direct authority to regulate privacy issues for UAVs.⁵⁷ For example, the FAA state that their mandate is to regulate civil aviation to promote and improve the safety and efficiency of flight in U.S. airspace.⁵⁸ Privacy issues raised with respect to the technology carried on UAVs,

such as technologies for surveillance, are deemed to be outside the FAA's mission unless the use of the technology affects the safe operation of the UAV.⁵⁹

In 2008, the GAO identified several obstacles to safe and routine operation of UAVs in the national airspace system in the U.S., which included sense and avoid deficiencies, and command and control vulnerabilities, and lack of regulations to govern safe operation. In its 2012 report, the GAO conveyed a relatively unchanged state of affairs with respect to those same safety concerns. The current restrictions on licensing and safety requirements mean that UAVs are usually limited to sparsely populated areas or controlled environments. In the UK the situation is similar; the Civil Aviation Authority has resisted the licensing of such aircraft in "normal" airspace due to fears of collisions.⁶⁰ Those technological deficiencies are the main roadblock to implementation in populated areas.

While aviation regulators are primarily concerned with ensuring the safety concerns posed by UAV flight are alleviated, only a few international self-regulatory codes of conduct have emerged to help ensure that drones are operated in a responsible and ethical manner. The Association for Unmanned Vehicle Systems International released an industry code of conduct with respect to the use of UAVs, which calls for responsible as well as safe use of the technology and makes very general statements that the UAS industry manufacturers and users will commit to a number of ethical standards under three themes: safety, professionalism and respect. It includes one statement regarding privacy, stating: "we will respect the privacy of individuals."⁶¹

Another code came from the International Association of Chiefs of Police Aviation Committee, which released *Recommended Guidelines for the use of Unmanned Aircraft*. While these guidelines acknowledge privacy as a concern, they also position privacy as running counter to the public safety benefits that UAVs promise:

"Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide. We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of our lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety."⁶²

The guidelines do suggest however, that "where there are specific and articulable grounds to believe that the [UAV] will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight."⁶³ It is likely that this statement reflects the instances where UAVs capture images over private property, rather than in public spaces.

While the mere acknowledgement of privacy within these codes is a positive step, they do not seem to go far enough. The fact remains that drones are licenced and regulated under an aviation safety framework concerned with safety, as opposed to the privacy implications of their use. In Canada, organizations using drones will be expected to go further to genuinely address the privacy implications of their use, and ensure that drones are used in accordance with privacy laws and guidelines.

PART FOUR: PRIVACY CONSIDERATIONS

As drones proliferate or become more routinely adopted and utilized by the public and private sectors, privacy implications and privacy regulations will have to be considered in the early stages of implementation.

Privacy Implications

The magnitude of the impact on privacy, including the extent and type of personal information that may be captured by UAVs, will depend largely on the purpose for which drones are used, the context and location of their use, as well as the type of technology mounted on them. The following section will discuss how drones could: a) change the nature of surveillance; and b) have an impact on expectations of privacy in public.

a) The changing nature of surveillance

UAVs are quite frequently compared to other forms of video surveillance or aerial surveillance using manned aircraft; however they also present unique privacy challenges due to their unique abilities and flexibility in the way in which they may collect personal information, ranging from acute and persistent tracking of individual activities to systematic surveillance of a wide area. There is a strong argument that UAVs may be a surveillance game-changer in three general areas: their attributes, payload technologies, and the manner in which they collect personal information.

UAV attributes

UAVs are a powerful surveillance tool and though there are often comparisons drawn between UAV surveillance and overhead surveillance by manned aircraft, or CCTV video surveillance cameras, the differences in the type of surveillance and observation need careful consideration. UAVs enable surveillance that is surreptitious, cheap, efficient, persistent and agile.

Unlike manned aircraft or CCTV cameras, the portable and mobile aspects of UAVs, coming at a reduced cost than manned aircraft, means that the potential for surveillance is more far-reaching: “the prospect of cheap, small, portable flying video surveillance machines threatens to eradicate existing practical limits on aerial monitoring and allow for pervasive surveillance.”⁶⁴ UAVs are not fixed in a specific location or vantage point and may raise unique privacy concerns because of their physical ability to track an individual’s activities or patterns of movement more persistently over time. Calo has written about the various attributes that demonstrate how UAVs are superior to humans, or fixed CCTV, in their ability to conduct surveillance. He notes, “enormous, unmanned drones can stay aloft, undetected, for days and relay surface activity across a broad territory...[s]maller drones can sweep large areas as well as stake out particular locations by hovering nearby and alerting a base upon detecting activity...due to their mobility, size, and sheer inhuman patience, robots permit a variety of otherwise untenable techniques.”⁶⁵

Although UAVs are visible in that they are a physical aircraft, certain attributes can make them a relatively covert form of surveillance. In practical terms, the portable, mobile and connected nature of UAVs might make it incredibly difficult for the public to know who the operators are. Murakami Wood argues that the ubiquity of surveillance is not only about how much surveillance occurs, but also the way in which it is becoming less and less obvious as it increases in quantity.⁶⁶ Moreover, they increasingly do not even look like surveillance technologies and do not even appear artificial.⁶⁷

Advancements in biomimetic technologies are going to transform the nature of surveillance. Biomimetics are machines that imitate naturally-occurring animals or plants (commonly birds, snakes and insects), and may be a significant concern for the future of unmanned surveillance technologies.⁶⁸

Payload technology

Surveillance technologies are reducing in size at the same time as they increase in power and range of activities.⁶⁹ Drones can be equipped with a full range of advanced surveillance technologies that could capture a wide range of detail and have a distinct ability to capture information dynamically and from unique vantage points.⁷⁰ Some of these technologies have the ability to capture data from great distances and through walls, and with a fine level of detail, for example the ability to capture the image of a person's face from miles away.

The sophistication of the technology that can be mounted as a payload on a drone will have different privacy implications. In the most basic terms, there will be different implications for privacy if a UAV is fixed with a high-powered camera versus a low-powered camera. Other technologies could take things a step further, such as thermal imaging devices, radar that can see through walls or biometric recognition technologies that could enable highly targeted surveillance or collection of unique information about the individuals below. Essentially, UAVs equipped with an array of sophisticated technology could “greatly magnify the human capacity to observe.”⁷¹ This is why they have been referred to as “unblinking eyes in the sky.”⁷²

Collection of personal information

Drones may change the nature of surveillance by virtue of the *type* of information they can collect. Law enforcement officials will often claim that UAVs are no different from a range of surveillance devices they already use, and simply facilitate routine police work or act as mere replacements for manned helicopters which are costly to run. The contrary position is that UAVs could actually be “transformative” in the manner in which they conduct surveillance and could “fundamentally alter the way ostensibly free societies are policed.”⁷³ Because of their technological capacity, the information that can be collected by UAVs could reveal “far more than the naked eye.”⁷⁴ For example, they could record the route and speed of every vehicle in the street, observe the movements of individual pedestrians, they can capture the precise moment when lights are turned on or off in a person's house.⁷⁵ Information captured by drones could then be correlated with other types of information, for example, our mobile devices, and then become an important ingredient in the growing digital record of everything we do.⁷⁶ “Drones might raise unique privacy concerns because of their ability to gather information from a particular “vantage point” which is distinguishable from the data we accumulate through our cellular phones or Internet searches.”⁷⁷

The vantage point, location and context of the collection will matter. For example, there may be a difference in the way people view surveillance by a close range targeted drone versus a high-altitude surveillance drone hovering over an entire city.⁷⁸ Moreover, a common feature of modern surveillance technologies is their automated and interconnected nature. Fleets of UAVs can be interconnected and augmented with analytics software that enable the mass tracking of vehicles and pedestrians around a large area.⁷⁹ Given the advances in analytics, and the desire of law enforcement to predict and preempt crime before it happens, it is easy to see how drones could contribute to the overall desire to collect enough information to enable predictions about crime patterns or prevent criminal activity before it occurs.

In their current form, Canada's privacy laws are primarily focused on the informational sphere of privacy, the protection of personal information that is collected by government and businesses. Drones may well be a discernible manifestation of how other spheres of privacy, such as spatial and physical privacy, continue to be

challenged by modern technologies. The Electronic Frontier Foundation (EFF) cautions that location-based digital services and technologies threaten to invade our “locational privacy”. In other words, the ability of an individual to move relatively anonymously in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use.⁸⁰ The convergence of technologies and systems are the enabling features of a world where information can be collected and linked together in such a way that it is possible to create an increasingly holistic picture of an individual’s activities, behaviours, and patterns of movement. UAVs could potentially be a key source in this trend to collect location information.

b) Expectations of Privacy in Public

The potential expansion of drones in domestic skies has spurred debates about their potential impact on diminishing expectations of privacy in public spaces. Whether they are operated by law enforcement or other public sector agencies, by private sector companies, or flown recreationally by citizens, the rise of drone use in Canada will likely intensify concerns about how to preserve and protect individual and collective privacy as people go about their daily lives.

The prospect that drones could eventually be deployed for a myriad of surveillance activities is often the most controversial proposed use. In particular, drones deployed by the public sector for surveillance raises questions regarding the proper balance between state obligations to keep people safe and to respect their privacy rights. It will only be a matter of time before the courts will have to consider the constitutional balance to be struck.⁸¹ Without a doubt, assessments about the “reasonableness” of drone surveillance, including reasonable expectations of privacy in public spaces, will be at the crux of the debate.

In a Congressional Research Service Report,⁸² Legislative Attorney Richard M. Thompson II argues that the “reasonableness” of drone surveillance will likely be informed by three factors: 1) location of the search, 2) the sophistication of the technology used, and 3) society’s conception of privacy in an age of rapid technological advancement. From a U.S. law perspective, he explains that reasonable expectations of privacy have a lot to do with the context or location in which the UAV surveillance takes place, such as if a target is at home, in their backyard, a public square, or near a national border. The technology also potentially has an impact on “reasonableness” if it enables law enforcement to see inside a home for example, or if it enables pervasive tracking and extensive data collection.⁸³ On the other hand, an area where individuals might find there is a reduced or “zero” expectation of privacy is travel in public places or near a U.S. border.⁸⁴

Thompson also points out that the reasonable expectations of privacy with regard to UAVs will be shaped by the public’s acceptance and the development of social norms about their use. He argues that the rarity of drone use may have some bearing on the analysis of what is “reasonable”, saying that in the current environment the general public would likely find it exceedingly unusual to see a drone flying over their home taking surveillance photographs. However this could begin to shift as UAVs proliferate and become more accessible to governments, private companies and even citizens. As drones become ever-present in our society, they can become “normalized” and therefore acceptable or accepted. He argues that if UAVs are first accepted for benign or favorable purposes, such as in research or in rescue operations, the public might more readily come to accept the use of drones for surveillance, or other purposes that have an impact on privacy particularly as we move towards a reality in which approximately 30,000 UAVs are planned to take to the skies in the next 20 years. That being said, there is already some evidence that the public is resistant to the use of UAVs for certain types of activities. A survey conducted this summer in the U.S. found that the American public supports drone use in certain circumstances, but is less enthusiastic about using them as part of routine law enforcement activity.⁸⁵

Drones and Canadian Privacy Laws and Guidance

In terms of the current situation in Canada so far, there has been no indication that drones are being used for general surveillance or to gather personal information.⁸⁶ However, Canada's privacy laws will apply to UAVs deployed by public or private sector organizations to collect and/or use personal information. Essentially, drone operations that involve the surveillance of Canadians or the collection of personal information are subject to the same privacy law requirements as with any other data collection practice.

Where UAVs are used for commercial aims, their use would be covered by the *Personal Information Protection Electronic Documents Act (PIPEDA)*, and subject to the same requirements as with any other data collection practice. It is a common misconception that a company does not require permission to take an individual's photograph in a public place.⁸⁷ The privacy protections in PIPEDA are there to ensure that people know when their image is being captured for commercial reasons – whether by photograph or video – and what it will be used for. PIPEDA requires consent as a general rule, subject to only limited and specific exceptions. Collection and use of personal information can only be for purposes that a reasonable person would consider appropriate in the circumstances and there should be a consideration for employing a less privacy-invasive means of obtaining the information.⁸⁸

Likewise, federal government departments intending to use drones will have to ensure their program activities are carried out in accordance with the *Privacy Act* and will have to ensure they undertake a Privacy Impact Assessment (PIA) in accordance with Treasury Board Directives.⁸⁹ Generally, when the public sector initiates new programs or activities impacting on privacy, there is an expectation that organizations carefully evaluate, and demonstrate, that the initiative is necessary to achieve a specific and legitimate purpose, that it is likely to be effective in achieving that purpose, that the intrusion on privacy is proportional to the benefit to be derived and that no other less privacy intrusive alternative would achieve the same purpose.⁹⁰ This is particularly important in the case of covert or intrusive public safety initiatives.⁹¹

Previously issued privacy guidance from the Office of the Privacy Commissioner of Canada (OPC) could be applicable and useful to organizations considering the use of drones for capturing images or video of individuals. The OPC's guidelines on the use of [overt](#) and [covert](#) video surveillance in the private sector as well as [Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities](#) are principles-based guidance that call on organizations to ensure surveillance activities are carried out in accordance with privacy obligations and responsibilities that exist in Canada.⁹²

A key challenge in the protection of privacy has frequently been the rapid development of new technologies. When it comes to the privacy implications of drones, a lot will depend on the purpose of their use and the scope of their implementation. Public awareness around the use of UAVs is often minimal, and citizens generally have few indications that UAVs are in use. Even in a hypothetical case where someone has an indication that their privacy may be violated by the operation of a UAV, it may prove challenging for individuals to produce sufficient evidence in support of their complaint under the *Privacy Act* or *PIPEDA*, particularly when dealing with unmarked or covert surveillance.⁹³

Furthermore, the advent of the smartphone has made model aircraft, and other such tools for surveillance, data, or image capture, a plausible option for recreational use by the public. The collection or use of personal information via model aircraft for personal purposes may reach beyond the scope of privacy law. Issues around "lateral surveillance" (citizens conducting surveillance on other citizens) is a growing phenomenon and recreational use of drones could further fuel this growing trend.

CONCLUSION: WHAT WILL HAPPEN NEXT?

The current state of domestic drone use in Canada is still fairly limited, given the existing aviation regulations and constraints on licencing. Some police forces in Canada have reported using them in limited circumstances, but there has been no indication that drones have been used for surveillance in Canada in either the public or private sectors. That being said, in view of the global focus on developing safe flight regulations, the increasing availability of the technology, and the projections for the global drone markets, the prospects are high for the proliferation of drone use in Canada in the foreseeable future.

Drones are often marketed and sold on the basis of the social benefits and conveniences they can afford for research, or for use in situations that are otherwise dangerous for human beings to intervene, such as fighting fires or studying hurricanes, or for search and rescue operations. It is true that some of the uses for drones may not be overly controversial, and thus it would be wrong to simply demonize the technology itself. However, as we look forward to a world that will inevitably include drones, it will be important to continue to reflect on the original question: will the proliferation of domestic drones use in Canada raise new concerns for privacy? There are many arguments to suggest that they will.

While the privacy implications of surveillance are fairly well known, drones could add an additional dimension to these privacy concerns by virtue of their mobility and persistence, and the range within which they can collect personal information using various advanced technologies mounted on board. This type of technological observation, with its inhuman persistence, is quite different from the type of observation that humans can do. Also, the proliferation of drones could trigger strong reactions or cause a chilling effect in public spaces if everyone felt watched, or potentially watched. It is conceivable that society's expectations of privacy in public could seriously erode if drone use for surveillance activities or any sort of data collection or tracking could become normalized over time as an accepted interference in our lives.



Of course, the flipside of the caution that drones could become normalized by society is an argument that the drone could actually help restore our mental model of a privacy violation, and in turn become a privacy catalyst.⁹⁴ As Calo pointed out, many people react to drones with intuitive concern because they represent “the cold, technological embodiment of observation.”⁹⁵ The physical presence and visibility of drones - to the extent that they *are* visible - could actually mean that people would feel observed regardless of how or whether the information was actually used, which could generate more resistance than the type of tracking that occurs in the digital/online sphere, where tracking and collection of personal information tends to be hard to visualize.

When it comes to the privacy implications of drones, a lot will depend on who is using them and for what purposes, the context and location of their use, the type of technology mounted on them and the extent and type of personal information that may be captured. As drones are acquired and put to use in Canada's public and private sectors, it will be important to circumscribe their use within an accountability structure that

ensures they are justified, necessary and proportional, and that the necessary checks and balances fundamental to a democratic society are in place to stave off proliferation of uses, abuses, and function creep. Canada's privacy laws will, and do apply to UAVs deployed by public or private sector organizations to collect and/or use personal information about citizens.

¹ Jack C. Chow. *The Case for Humanitarian Drones*, Canadian International Council, December 12, 2012.

<http://opencanada.org/features/the-think-tank/essays/the-case-for-humanitarian-drones/>

² Greg McNeal. "A Primer on Domestic Drones: Legal, Policy, and Privacy Implications," *Forbes*, April 10, 2012.

<http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>

³ *Canadian Aviation Regulations* (CARs), s. 102.01.

<http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf>

⁴ Federal Aviation Administration (FAA). Definition of "unmanned aircraft system"

http://www.faa.gov/about/initiatives/uas/uas_faq/#Qn1

⁵ Council of the European Union. *Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*, Working Paper (13438/12), September 6, 2012.

<http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf>

⁶ UVS International. Glossary of Terms.

http://www.uvs-international.org/index.php?option=com_docman&task=doc_view&gid=1988&Itemid=43 (link valid at time of writing)

⁷ CARs, s. 101.01.

<http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf>

⁸ Government Accountability Office. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. United States Government Accountability Office, Report to Congressional Requestors, GAO-12-981, September 2012.

<http://www.gao.gov/assets/650/648348.pdf>

⁹ *Ibid.*

¹⁰ For example, Korean researchers are working to teach robots how to hide from and sneak up on a subject, according to Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*.

American Civil Liberties Union (ACLU), 2011, p 4.

<https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

¹¹ These generally come from Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011, p 4.

<https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

¹² General Atomics. <http://www.ga-asi.com/products/aircraft/index.php>

¹³ Declan McCullagh. "Homeland Security: Let's be clear about aerial drone privacy," CNET News, February 22, 2013.

http://news.cnet.com/8301-13578_3-57570751-38/homeland-security-lets-be-clear-about-aerial-drone-privacy/

¹⁴ Ottawa Citizen. "Canadian Military Intends To Spend \$1 Billion On Armed Drones", July 8, 2012.

<http://www.ottawacitizen.com/news/Canadian%2Bmilitary%2Bintends%2Bspend%2Bbillion%2Barmed%2Bdrones/7048045/story.html>
(link valid at time of writing)

¹⁵ National Geographic. "Pictures: Drones Take on Hurricanes, Environment Work."

<http://news.nationalgeographic.com/news/2012/09/pictures/120921-hurricane-drones-nasa-usgs-environment-science/>

¹⁶ Nevins, Joseph. "Robocop: Drones at Home". Boston Review, 2011.

<http://www.bostonreview.net/robocop-joseph-nevins-drones-at-home>

¹⁷ Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011, p 4.

<https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

¹⁸ Amazon. <http://www.amazon.com/Parrot-AR-Drone-Quadricopter-Controlled-Android/dp/B007HZLLOK>;
<http://ardrone2.parrot.com/>

¹⁹ David Murakami Wood. *Vanishing Surveillance: Why Seeing What is Watching Us Matters*. A paper prepared for the Office of the Privacy Commissioner of Canada July 29, 2011.

http://www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp

²⁰ Greg McNeal. "A Primer on Domestic Drones: Legal, Policy, and Privacy Implications," *Forbes*, April 10, 2012.

<http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>

²¹ Dion Nissenbaum. "From Battlefield to the Border," *Wall Street Journal*, Aug 13, 2012.

<http://online.wsj.com/article/SB10000872396390443404004577581751184540464.html?KEYWORDS=mexico#articleTabs%3Darticle>

²² Rachel L. Finn and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review*, Vol. 28, No. 2, April 2012, pp. 184-194.

<http://www.sciencedirect.com/science/article/pii/S0267364912000234>

²³ Examples come from Stanley, J. And Crump, C., 2011. *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011; and Richard M. Thompson II *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Congressional Research Service (CRS) Report, September 6, 2012. (The report was subsequently re-released on April 3, 2013).

<http://www.fas.org/sgp/crs/natsec/R42701.pdf>

²⁴ "Unblinking eyes in the sky," *The Economist*. May 3, 2012.

<http://www.economist.com/node/21548485>

²⁵ Transport Canada. *Unmanned Aircraft Vehicles (UAV)*.

<http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm>

²⁶ For example, UAVs carrying atmospheric sensors can take targeted measurements to improve the ability to predict weather and climate conditions. From Morgan Bettex. "3 Questions : Nicholas Roy on deploying drones in U.S. skies," *MIT News*, 21 July 2010. <http://web.mit.edu/newsoffice/2010/3q-roy-uav-0722.html>

²⁷ These applications are noted in "Unblinking eyes in the sky," *The Economist*, May 3, 2012

(<http://www.economist.com/node/21548485>) and *Privacy and Drones: Unmanned Aerial Vehicles*, published by the Information and Privacy Commissioner of Ontario, August 2012.

<http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>

²⁸ Transport Canada's UAV Working Group Final Report (2007).

<http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uavworkinggroup-2266.htm#11.1%20indent-left5>

²⁹ Council of the European Union. *Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*, Working Paper (13438/12), September 6, 2012.

<http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf>

³⁰ David Canton, "Tech Watch: Drones offer whole new candid camera," *London Free Press*, 14 October 2012.

<http://www.lfpress.com/2012/10/14/tech-watch-drones-offer-whole-new-candid-camera>

³¹ Council of the European Union. *Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*, Working Paper (13438/12), September 6, 2012.

<http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf>

-
- ³² Suggestion that Google may be interested in using drones for the next iteration of “street-view,” from Forbes. Greg McNeal. “A Primer on Domestic Drones: Legal, Policy, and Privacy Implications,” *Forbes*, April 10, 2012.
<http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>
- ³³ Greg McNeal. “A Primer on Domestic Drones: Legal, Policy, and Privacy Implications,” *Forbes*, April 10, 2012.
<http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>
- ³⁴ “Unblinking eyes in the sky,” *The Economist*. May 3, 2012.
<http://www.economist.com/node/21548485>
- ³⁵ Government Accountability Office. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. United States Government Accountability Office, Report to Congressional Requestors, GAO-12-981, September 2012. <http://www.gao.gov/assets/650/648348.pdf>
- ³⁶ Jennifer Quinn. “Police drones sparks debate over personal privacy,” *The Toronto Star*, February 5, 2013.
http://www.thestar.com/news/world/2013/02/05/privacy_vs_security_when_does_the_use_of_drones_cross_the_line.html
- ³⁷ *Ibid.*
- ³⁸ The Standing Senate Committee on National Security and Defense - Evidence, April 23, 2012.
<http://www.parl.gc.ca/content/sen/committee/411/SECD/49470-E.HTM>
- ³⁹ *Ibid.*
- ⁴⁰ “Unblinking eyes in the sky,” *The Economist*. May 3, 2012.
<http://www.economist.com/node/21548485>
- ⁴¹ The Parrot AR Drone is probably the most popular hobbyist/toy drone, and it is currently available at places such as the Apple Store, The Source, Toys “R”Us, Best Buy, and even in the SkyMall Catalogue.
- ⁴² Always Innovating Inc. www.alwaysinnovating.com
- ⁴³ Julian Horsey. “MeCam Flying Camera Smartphone Copter With Auto Follow Feature Unveiled (video),” *Geeky Gadgets*, January 25, 2013. <http://www.geeky-gadgets.com/mecam-flying-camera-smartphone-copter-with-auto-follow-feature-unveiled-video-25-01-2013/>
- ⁴⁴ CARs s.602.41.
<http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf>
- ⁴⁵ Transport Canada’s website explains that [UAVs are regulated using SFOC](#). The air operator certificate is not mentioned. The requirements for obtaining an air operator certificate are contained in Part VII of the CARs. An air operator certificate is issued to a person or company involved in the operation of aircraft for Commercial Air Service, including Aerial work (CARs 702), Air Taxi (CARs 703), Commuter (CARs 704) or Airline (CARs 705). It is unclear at this time how the air operator certificate would be used to regulate UAV flight.
<http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm>
- ⁴⁶ CARs s.623.65(d).
<http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf>
- ⁴⁷ As noted by Lt.-Gen. Semianiw in the Standing Senate Committee on National Security and Defense - Evidence, April 23, 2012.
<http://www.parl.gc.ca/content/sen/committee/411/SECD/05EVB-49470-E.HTM>
- ⁴⁸ Transport Canada Staff Instruction Manual for reviewing and processing an application for an SFOC for the operation of a UAV. Staff Instruction (SI) No. 623-001.
<http://www.tc.gc.ca/eng/civilaviation/opssvs/managementservices-referencecentre-documents-600-623-001-972.htm#e8-20>

⁴⁹ These are contained in Transport Canada's Staff Instruction Manual for reviewing and processing an application for an SFOC for the operation of a UAV. Staff Instruction (SI) No. 623-001.

http://www.tc.gc.ca/media/documents/ca-opssvs/623-001_1.pdf

⁵⁰ Greg McNeal. "A Primer on Domestic Drones: Legal, Policy, and Privacy Implications," *Forbes*, April 10, 2012.

<http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>

⁵¹ Government Accountability Office. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. United States Government Accountability Office, Report to Congressional Requestors, GAO-12-981, September 2012. <http://www.gao.gov/assets/650/648348.pdf>

⁵² Europe 2020 is the European Union's ten-year economic growth strategy.

http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/index_en.htm

⁵³ Council of the European Union. *Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*, Working Paper (13438/12), September 6, 2012.

<http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf>

⁵⁴ Peter van Blyenburgh. "Towards a European Strategy for the Development of Civil Applications of RPAS" *UAS Vision*, September 7, 2012.

<http://www.uasvision.com/2012/09/07/towards-a-european-strategy-for-the-development-of-civil-applications-of-rpas/>

⁵⁵ *Unmanned Aircraft Systems (UAS) Work Plan*, Canada's Economic Action Plan.

<http://actionplan.gc.ca/en/page/rcc-ccr/unmanned-aircraft-systems-uas-work-plan>

⁵⁶ Transport Canada "promotes safe, secure, efficient and environmentally-responsible transportation"; FAA's mission is to "provide the safest, most efficient aerospace system in the world".

⁵⁷ Government Accountability Office. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. United States Government Accountability Office, Report to Congressional Requestors, GAO-12-981, September 2012, p 38.

<http://www.gao.gov/assets/650/648348.pdf>

⁵⁸ Federal Aviation Authority

http://www.faa.gov/about/safety_efficiency/

⁵⁹ Government Accountability Office. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. United States Government Accountability Office, Report to Congressional Requestors, GAO-12-981, September 2012, p 38. <http://www.gao.gov/assets/650/648348.pdf>

⁶⁰ Joseph Nevins. "Robocop: Drones at Home," *Boston Review*, 2011.

<http://www.bostonreview.net/robocop-joseph-nevins-drones-at-home>

⁶¹ Association for Unmanned Systems International (AUSVI) *Unmanned Aircraft System Operations Industry "Code of Conduct."*

<http://www.auvsi.org/conduct>

⁶² International Association of Chiefs of Police Aviation Committee. *Recommended Guidelines for the use of Unmanned Aircraft*.

http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf

⁶³ *Ibid.*

⁶⁴ Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011.

<https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

⁶⁵ Ryan Calo, "Robots and Privacy," in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds) Cambridge: MIT Press, forthcoming. <http://ssrn.com/abstract=1599189>

⁶⁶ David Murakami Wood. *Vanishing Surveillance: Why Seeing What is Watching Us Matters*. A paper prepared for the Office of the Privacy Commissioner of Canada, July 29, 2011. http://www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp

⁶⁷ *Ibid.*

⁶⁸ For example, certain research projects are being developed and tested and in many cases funded by US Defence Research Projects Agency (DARPA), such as AeroVironment's "Nano Hummingbird" (<http://www.avinc.com/nano/>), from Murakami Wood, David. *Vanishing Surveillance: Why Seeing What is Watching Us Matters* (http://www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp). A paper prepared for the Office of the Privacy Commissioner of Canada, July 29, 2011.

⁶⁹ David Murakami Wood. *Vanishing Surveillance: Why Seeing What is Watching Us Matters*. A paper prepared for the Office of the Privacy Commissioner of Canada, July 29, 2011. http://www.priv.gc.ca/information/research-recherche/2011/wood_201107_e.asp

⁷⁰ *Privacy and Drones: Unmanned Aerial Vehicles*, published by the Information and Privacy Commissioner of Ontario, August 2012. <http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>

⁷¹ Ryan Calo, "Robots and Privacy," in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds) Cambridge: MIT Press, forthcoming. Available at: <http://ssrn.com/abstract=1599189>

⁷² "Unblinking eyes in the sky," *The Economist*. May 3, 2012. <http://www.economist.com/node/21548485>

⁷³ Joseph Nevins. "Robocop: Drones at Home," *Boston Review*, 2011. <http://www.bostonreview.net/robocop-joseph-nevins-drones-at-home>

⁷⁴ Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011. <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

⁷⁵ John Villasenor. "High-altitude drones: Coming to a sky near you," *Scientific American*, February 24, 2012. <http://blogs.scientificamerican.com/guest-blog/2012/02/24/high-altitude-surveillance-drones-coming-to-a-sky-near-you/>

⁷⁶ Quoting John Villasenor in Stanley, J. And Crump, C., *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011. <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

⁷⁷ Citing John Villasenor, a senior fellow at the Brookings Institution, in Greg McNeal. "A Primer on Domestic Drones: Legal, Policy, and Privacy Implications," *Forbes*, April 10, 2012. <http://www.forbes.com/sites/gregorymneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/>

⁷⁸ John Villasenor. "High-altitude drones: Coming to a sky near you," *Scientific American*, February 24, 2012. <http://blogs.scientificamerican.com/guest-blog/2012/02/24/high-altitude-surveillance-drones-coming-to-a-sky-near-you/>

⁷⁹ Stanley, J. And Crump, C. *Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft*. American Civil Liberties Union (ACLU), 2011. <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>

⁸⁰ Andrew J. Blumberg and Peter Eckersley. "On Locational Privacy, how to avoid losing it forever," Electronic Frontier Foundation (EFF), August 2009. <https://www.eff.org/wp/locational-privacy>

⁸¹ Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Congressional Research Service (CRS) Report, September 6, 2012. (The report was subsequently re-released on April 3, 2013.) <http://www.fas.org/sgp/crs/natsec/R42701.pdf>

⁸² *Ibid.*

⁸³ As noted in the GPS tracking case *Jones*, Surveillance in public may cross the line to unreasonable if it is pervasive tracking in public including the length of time an individual is tracked and the extent of the data collection. From Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Congressional Research Service (CRS) Report, September 6, 2012. (The report was subsequently re-released on April 3, 2013.) <http://www.fas.org/sgp/crs/natsec/R42701.pdf>

⁸⁴ *Ibid.*

⁸⁵ Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Congressional Research Service (CRS) Report, September 6, 2012. (The report was subsequently re-released on April 3, 2013.) <http://www.fas.org/sgp/crs/natsec/R42701.pdf>

⁸⁶ As noted by Assistant Commissioner Chantal Bernier to CBC, “Drones work the skies for police, scientists, media.” *CBC News*. <http://www.cbc.ca/news/technology/story/2012/03/22/technology-the-current-civilian-drones.html>

⁸⁷ Fact Sheet prepared jointly by the Offices of the Information and Privacy Commissioners of Alberta and British Columbia and the Commission d'accès à l'information du Québec, and the Privacy Commissioner of Canada (OPC), *Captured on Camera: Street-level imaging technology, the Internet and you*. http://www.priv.gc.ca/resource/fs-fi/02_05_d_39_prov_e.asp

⁸⁸ “Flying robots – not just for war anymore,” *Privacy Scan*, published May 4, 2012, by the Law Office of Kris Klein. <http://www.privacyscan.ca/issues/2012/may-4-2012-flying-robots-not-just-for-war-anymore/>

⁸⁹ Treasury Board Secretariat (TBS) Directive on Privacy Impact Assessment. Effective April 2010. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308>

⁹⁰ See Expectations: a Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada, OPC Guidance, March 2011. http://www.priv.gc.ca/information/pub/gd_exp_201103_e.asp

⁹¹ As indicated in OPC Guidance: *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*, November 2010. http://www.priv.gc.ca/information/pub/gd_sec_201011_e.asp

⁹² Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities, March 2006. (http://www.priv.gc.ca/information/guide/vs_060301_e.asp); Guidelines on the use of Overt Video Surveillance in the Private Sector, March 2008 (http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp); Guidelines on the use of Covert Video Surveillance in the Private Sector, March 2008 (http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.asp)

⁹³ See OPC's website, *How to file a Privacy Complaint* (http://www.priv.gc.ca/complaint-plainte/index_e.asp); Section 34, *Privacy Act*; and Section 12, *Personal Information Protection and Electronic Documents Act (PIPEDA)*

⁹⁴ Ryan Calo, *The Drone as Privacy Catalyst*, 64 *Stanford Law Review Online* 29, 2011. <http://www.stanfordlawreview.org/online/drone-privacy-catalyst>

⁹⁵ *Ibid.*