BLOCK G

PRIVACY & SECURITY CONSULTING

Watching Below:

Dimensions of Surveillance-by-UAVs in Canada

This page has intentionally been left blank.

© 2013 BlockG Privacy and Security Consulting. All rights reserved.

Electronic version first published at www.blockg.ca in Canada in 2013 by BlockG Privacy and Security Consulting.

BlockG Privacy and Security Consulting logo designed by Karen Yen of Can Poeti Branding and Design.

Document version 1.2

The materials contained in this report are copyright to BlockG Privacy and Security Consulting. All brand and product names and associated logos contained within this report belong to their respective owners and are protected by copyright. Under no circumstance may any of these be reproduced in any form without the prior written agreement of their respective owners.

Information presented in this document is for research and educational purposes only. These materials do not constitute solicitation or provision of legal advice. BlockG Privacy and Security Consulting makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Nothing herein should be used as a substitute for the legal advice of competent counsel.

CONTENTS

Executive Summary

Unmanned aerial vehicles (UAVs) are increasingly moving from military combat theatres to domestic airspaces. UAVs are used for a brand range of domestic applications, including as children's toys, aids to facilitate visually spectacular movie scenes, and valuable environmental assessment technology. UAVs are also used increasingly by law enforcement agencies across a range of policing and emergency management operations. The goals of this report are to contextualize the current uses of this last type of UAV in Canada and to consider the drawbacks, laws, and politics that are influencing the adoption of UAVs by Canadian authorities. The report considers where work is needed to develop democratically accountable and privacy-protective UAV policies in Canada. We draw on large quantities of documents received through access to information and privacy requests. Using information from these documents as well as from expert interviews, we identify key stakeholder groups that are developing UAV policies to meet law enforcement expectations and indicate the need to adequately preserve Canadian citizens' and residents' reasonable expectations of privacy.

This report is divided into six sections. **Section One** outlines the methodology we adopted in the course of developing this report and identifies the range of sources that we relied upon in the report. In **Section Two,** we identify UAV-based technologies and discuss how these technologies can be used. As part of this process, we differentiate between anticipated uses of the vehicles versus the ways in which Canadian law enforcement bodies presently expect to integrate UAVs into their existing fields of practice. **Section Three** outlines the reasons that aerial surveillance is a potentially significant new form of police surveillance, focusing on the particularities of wide-spectrum aerial sensing systems that monitor terrestrial space more effectively than land-based alternatives. While we acknowledge the potential usefulness of UAVs for policing, in **Section Four** we also recognize that UAVs are currently vulnerable in the following ways: third parties can intercept communications, third parties can disrupt flight operations, and operator errors can lead to crashes.

After outlining how and why UAVs are adopted and the potential drawbacks of the vehicles from safety and privacy perspectives, we move to discuss the emerging policy landscape in Canada. In **Section Five,** we identify relevant Canadian policy, regulations, and law that mediate how authorities can adopt UAVs. Our central conclusion is that the policy development process remains nascent and informal: while Transport Canada has guidelines for using UAVs, the institution focuses on safety over privacy, and police

working groups have yet to establish a coherent, cross-national policy for authorities' uses of the vehicles. Moreover, typical 'privacy actors,' such as the federal and provincial privacy commissioners of Canada, academics attendant to privacy issues in Canada, and Canadian civil liberties groups, have been late in formally taking up UAVs as pressing policy issues. We suggest that the policy network will soon expand as commissioners, academics, and members of civil society have recently begun expressing interest in how authorities are using or are intending to use UAVs in Canada.

The final section, **Section Six**, identifies a set of key issue areas and offers associated recommendations. First, UAVs must be proven safe for law enforcement purposes before being adopted by law enforcement authorities (LEAs). Second, LEAs must be genuinely mindful of the privacy considerations that are linked to UAVs and, as part of this, must work proactively with privacy commissioners and interested members of civil society to ensure that Canadians are satisfied with the privacy protections that are incorporated into the use of UAVs in Canada. Third, Canadian LEAs should be explicit about how they are currently using or training with UAVs and about the future purposes to which they intend to use UAVs. Moreover, LEAs should clearly consult with Canadians to ensure that their operations resonate with Canadians' own interests in how UAVs are used. Finally, the existing uneven governance framework needs improvement: working parties should be formally set up to integrate discussions across provincial/federal lines of responsibility in order to establish a common, high-quality degree of oversight and regulation of UAVs. We conclude the section by identifying areas where subsequent policy research should be conducted.

UAVs are flying in Canadian skies in exponentially increasing numbers. At the moment, policy makers are well positioned to guide the use of UAVs proactively. Policy makers should clarify appropriate uses of UAVs in a political climate that is free from untoward events, such as major equipment failure, that might distract from the host of privacy and surveillance issues that are implicated in the use of UAV technology. The time for such well-balanced policy making is now, and currently all stakeholders have an opportunity to work to ensure that Canadians' safety and privacy are protected while ensuring that UAVs operate under a robust and comprehensive UAV governance framework.

Introduction

Unmanned Aerial Vehicles (UAVs) are not a particularly new phenomenon. Initially meant for use as unmanned aerial torpedoes in the First World War, they have subsequently been developed and deployed for military, civilian, and corporate purposes. From conducting military surveillance to becoming children's toys and from facilitating visually spectacular movie scenes to conducting environmental analyses, UAVs are being deployed for wide-ranging monitoring, surveillance, and interdiction purposes. Though UAVs have largely been used for military purposes, citizens and public authorities alike are using them increasingly in domestic environments.

In the domain of domestic governance, UAVs are currently used for "wildlife emissions monitoring, weather forecasting, topographical mapping, wildlife management, and traffic surveillance."[1] Moreover, the vehicles are regarded as offering new capabilities for law enforcement authorities (LEAs), with one authority stating that "[n]ot since the Taser has a technology promised so much for law enforcement."[2] These promises arise because UAV systems can carry a host of instruments and can be deployed for a variety of policing functions. UAVs are seen as 'force multipliers' for LEAs because of their range of uses. LEAs value such multipliers because authorities are now expected to respond to domestic criminal issues, engage in counter-terrorism and border security initiatives, as well as take part in emergency/disaster management.

LEAs are also interested in using UAVs to identify and forestall public order disturbances and implement control tactics during criminal events. Rich aerial surveillance data enhances 'actuarial', or predictive, policing by augmenting existing terrestrial surveillance capabilities. Such policing practices depend on software systems using "advanced algorithms to allow police agencies to predict locations where a certain type of crime is likely to occur and direct appropriate resources to those areas."[3] Police can develop risk probabilities "and then manage populations or eliminate network nodes considered to exceed acceptable risk thresholds"[4] on the basis of

[1] Travis Dunlop. (2009). "We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search," *South Texas Law Review* 51 (73). Pp. 179.
[2] Ben Miller, quoted in Peter Finn. (2011). "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *The Washington Post*, January 23, 2011. Accessed June 4, 2013. http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.
[3] National Institute of Justice. (2011). "The Predictive Policing Symposium: A Strategic Discussion," *Geography & Public Safety* 2(4). Pp. 2.
[4] Tyler Wall and Torin Mohahan. (2011). "Surveillance and violence from afar: The politics of drones and liminal security-scapes," *Theoretical Criminology* 15(3): 239-254. Pp. 240.

collected data and its subsequent analysis. By managing the population based on risk analysis, authorities can ensure that order is maintained, not just restored.

This report explores how LEAs are deploying UAVs in domestic settings and focuses on how UAVs enable new surveillance capabilities that could be directed toward Canadian citizens and residents. In the **first section,** we briefly discuss our methodology and note the key sources of data that we used to prepare this report. The **second section** discusses how UAVs are being equipped with technologies to conduct human, environmental, and vehicular surveillance. The **third section** explores the ramifications of using UAVs to conduct surveillance. The **fourth section** considers how UAVs might fail in the course of their surveillance practices. The section asserts that operational, safety, and privacy challenges are tied to LEAs' proposed uses of the vehicles.

The **fifth section** identifies policies, regulations, and laws that most clearly pertain to Canadian authorities' uses of UAVs. In this section, we also identify key actors in the Canadian policy network who are addressing 'UAV issues' and their respective roles and positions. The **sixth section** of this report offers recommendations and specific items that policy analysts would be advised to take up in their own work. We then conclude by summarizing key points raised by our report.

Section One – Methodology

We have adopted a qualitative, small-N, methodology for this report and draw predominantly on North American data sources. Throughout, we depended on primary documents, elite-level interviews, and desk research to collect data about UAV usage in North America and Canada, in particular. Primary documents were predominantly received following Access to Information and Privacy (ATIP) requests to branches of the Federal Government of Canada. Specifically, we used documents from Transport Canada (TC), Ministry of Justice, the Department of National Defence (DND), the Royal Canadian Mounted Police (RCMP), and Canadian municipal law enforcement agencies to clarify the number of UAVs that Canadian authorities have adopted, the range of private authorities and technologies involved, as well as UAV's current and intended uses. A significant portion of the approximately 500 pages of records that we obtained through ATIP spanned policy discussions that took place between 2006 and 2012. ATIP records included policy documents, public presentations, email files, policy documents concerning operational and definitional standards pertaining to UAVs, corporate contracts, and product information on UAV technologies that are used currently.

Limited elite-level interviews were conducted with members of the Canadian policing community to gauge their interest in UAV technologies, as well as to explore the policies and practices that have been and are being developed as UAVs are deployed in Western Canada. Interviews were semi-structured and conducted during the winter of 2012 with municipal-level police officers. Selected officials were chosen because of their positions relative to training and implementing UAV technologies in their local detachments. Officials are not specifically identified in this report.

Finally, desk research provided empirical details of UAV uses as well as scholarly analyses of existing policies, regulations, laws that intersect with UAV practices, and drivers of UAV deployments. Unfortunately, much of the scholarly literature focuses on American and European domestic UAV activity; scant focused work exists on the Canadian situation. Regardless, we drew from governmental research reports, journalistic accounts, published scholarly work, and articles produced by private consulting firms as appropriate.

Section Two – UAV Technologies and Uses

In the United States (US), the Federal Aviation Authority (FAA) estimates that up to 30,000 UAVs will be flying in American skies within 20 years.[5] The number of unmanned aircraft that will have received FAA approval speaks to the commercial and LEA interest in UAVs' capabilities, capabilities that are attributable to the immense number of technical systems that have been designed to 'attach' to these aerial platforms for monitoring, surveillance, and interdiction purposes. In addition to the appeal of highly variable operational functionality, UAVs are relatively inexpensive compared to manned aerial vehicles. In what follows, we first outline technical capabilities of UAVs to underscore the range of their potential uses. We then outline how North American authorities are using or would like to use of these capabilities. Together, this discussion clarifies how UAVs are currently being used and suggests that UAVs are at only the earliest stages of being integrated into policing strategies.

In the public sector, a range of federal, state/provincial, and municipal authorities use UAVs. The vehicles are used for reconnaissance, intelligence-gathering, object targeting, and encompass public safety operations, law enforcement, customs and border patrol, emergency services, and commercial aerial imaging.[6] In more specific terms, public authorities are presently using UAVs to detect radiation in hazardous material situations, monitor hostage situations, provide tactical support, detect improvised explosives, locate missing persons, as well as assist in firefighting.[7] These vehicles are, in essence, being integrated into a wide range of public bodies' routine operations.

While UAV systems can serve in a variety of operational contexts, they are most commonly "outfitted with high-powered cameras, thermal imaging devices, license plate readers, and laser radar (LADAR)."[8] Such attachments are useful for LEAs because, in many cases, aerial surveillance "provides better perspective" than ground-based

---

[5] Federal Aviation Association. (2010). "FAA Aerospace Forecast Fiscal Years 2010-2030," *Federal Aviation Authority*, 2010. Accessed June 4, 2013. Available at: http://www.faa.gov/data_research/aviation/aerospace_forecasts/2010-2030/media/2010%20Forecast%20Doc.pdf.

[6] Richard M. Thompson II. (2013). "Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," *Congressional Research Service*. Published April 3, 2013. Pp. 3.

[7] Richard M. Thompson II. (2013). "Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," *Congressional Research Service*. Published April 3, 2013. Pp. 3

[8] Richard M. Thompson II. (2012). "Dones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," *Congressional Research Service*. Published September 6, 2012. Pp. 3-4.

surveillance. In particular, UAVs create the possibility for LEAs to "cover a large area and focus resources on current problems. [They] have the advantage of being mobile, and [they are] able to be present in both time and space."[9] Moreover, these vehicles are often designed to evaluate a scene and juxtapose it against a preprogrammed normative definition of what an orderly scene 'ought to' look like. It is on the basis of applying normative logics to what is monitored that UAVs can identify complex patterns of behaviour, including "vehicle overtaking, traversing of intersections, [and] parking lot activities."[10] Furthermore, UAV imaging systems can be integrated with ground-based sensors that, when triggered, activate UAV-mounted surveillance equipment.[11]

The law enforcement potentials for LEA UAVs are significant; advocates of these vehicles imagine a future when swarms of surveillance drones are deployed to cordon off or surround buildings or city blocks.[12] One document accessed by *The Guardian* suggested that British authorities want to use UAVs for "[detecting] theft from cash machines, preventing theft of tractors and monitoring antisocial driving," while another states that the aircraft could be used for "road and railway monitoring, search and rescue, event security and covert urban surveillance." Another document that the newspaper accessed suggested using UAVs to "combat "fly-posting,[13] fly-tipping,[14] abandoned vehicles, abnormal loads, [and] waste management"."[15] These are just some of the 'modest' visions of how UAVs could be incorporated into policing practices. While such visions do not necessarily indicate what the vehicles *can* accomplish or how they *will* be used, such visions reveal some authorities' *imaginaries* linked with UAVs.

There is, of course, a difference between the potential uses of UAVs for surveillance and interdiction and their current use by LEAs in the United States or Canada. Importantly, the types of missions or operations that involve UAVs are highly dependent on the 'class' of UAV that is available to the relevant LEA: specific vehicles might have been

[9] Anuj Puri. (2005). "A Survey of Unmanned Aerial Vehicles (UAV) for Traffic Surveillance," *Department of computer science and engineering, University of South Florida*. Pp. 2.
[10] Anuj Puri. (2005). "A Survey of Unmanned Aerial Vehicles (UAV) for Traffic Surveillance," *Department of computer science and engineering, University of South Florida*. Pp. 2.
[11] Rachel L. Finn and David Wright. (2012). "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review* 28 (2012): 185-194.
[12] Michael Brooks. (2012). "The Drone Age," *New Scientist* Vol. 216(2894): 42.
[13] Fly-posting refers to 'guerilla marketing' tactics that involve pasting posters to walls without permission.
[14] Fly-tipping refers to the illegal dumping of waste or rubbish.
[15] Paul Lewis. (2010). "CCTV in the sky: police plans to use military-style spy drones," *The Guardian*, January 23, 2010. Accessed June 4, 2013. Available at: http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones.

purchased for a particular purpose but can subsequently be used for other, not previously specified, missions.

In general terms, there are three main classes of UAVs: micro and mini, tactical, and strategic vehicles. Micro and mini vehicles are meant for low-altitude flights and are designed to operate in cities and buildings. Whereas micro UAVs can weigh as little as 100 grams, mini UAVs weigh less than 30 kilograms.[16] The result is that micro and mini UAVs are principally used for civilian and commercial applications, although some LEAs have found policing uses, such as providing close tactical support to officers in emergency situations, for this class of UAV.

Tactical and strategic UAVs, in contrast, are heavier and capable of longer flight times and carrying broader operational payload capabilities than mini- and micro-UAVs. Tactical UAVs weigh up to 1,500 kilograms and fly as high as 8,000 meters. They have traditionally been used for military operations and often rely on satellite links to communicate with ground control stations. Strategic UAVs are also principally used by the military and can weigh up to 12,000 kilograms and fly at an altitude of up to 20,000 meters. Where strategic UAVs are powered by solar or other renewable energy, they can remain airborne for considerable periods of time.[17]

The different capabilities of these kinds of vehicles afford varying use-cases to LEAs. Authorities might develop heightened urban awareness capabilities when using micro or mini vehicles, though such awareness might be limited by the UAV's operational payload weight capacity and the expense of miniaturized surveillance equipment. Specifically, the cost of miniaturized equipment might prohibit using UAVs for highly divergent missions that might rely on different equipment in the near future. Despite operational limitations and expense, local authorities are often excited by the prospect of adding even smaller UAVs to their policing arsenals. As recognized by Wall and Monahan, Houston police saw UAVs as a way to facilitate covert police actions and, potentially, even to write traffic tickets. Analysts suggest that Las Vegas might have been using UAVs since 2007, and confidential documents have revealed how UAVs could be used to monitor 'special events' and provide data to fusion-centres.[18] UAVs

[16] Ann Cavoukian. (2012). "Privacy and Drones: Unmanned Aerial Vehicles," *Information and Privacy Commissioner, Ontario, Canada*. Published August 2012. Pp. 6.
[17] Ann Cavoukian. (2012). "Privacy and Drones: Unmanned Aerial Vehicles," *Information and Privacy Commissioner, Ontario, Canada*. Published August 2012. Pp. 6-7.
[18] Tyler Wall and Torin Mohahan. (2011). "Surveillance and violence from afar: The politics of drones and liminal security-scapes," *Theoretical Criminology* 15(3): 239-254. Pp. 240. Such centres are ostensibly tasked with collecting information from federal, state, and municipal levels to tease out relevant intelligence findings for various level of government.

were used in 2007 to monitor political rallies in New York and Washington, DC,[19] and, in North Carolina, to monitor motorcycle riders and detect marijuana fields using infrared cameras.[20] In general, UAVs' abilities to remain airborne and capture images of terrestrial subjects lets LEAs monitor crowd movements as well as track individuals moving through dense spaces that are sometimes hard for officers to navigate. Trials are in progress to test using UAVs to identify and respond to gun shots,[21] find criminal suspects, and photograph crime scenes.[22]

In the United States, UAVs have been also used to monitor undocumented migration across the Arizona-Mexico border and smuggling of both drugs and people along the US-Mexico border. UAVs have helped the Department of Homeland Security save funds - Predator UAVs cost $4.5 million compared to manned aircraft costing $36 million or Blackhawk helicopters costing $8.6 million - as well as reduce potential operator casualties.[23] As of 2010, US Customs and Border Protection has operated six unarmed Predators[24] and, between 2010 and 2013, the agency has flown its UAVs over 500 times in support of other government agencies. In over 100 cases, these flights were for a "Department of Justice component including FBI, DEA and US Marshals," as well as for "the Grand Forks SWAT, the North Dakota Narcotics Task Force, the Bureau of Indian Affairs, the Arizona Department of Public Safety, the Minnesota Drug Task Force, and several branches of the military."[25]

Some American domestic law enforcement agencies currently use UAVs - often micro- or mini-UAVs that can stay aloft for only a few hours, at most[26] - for close tactical

---

[19] John W. Whitehead. (2010). "Drones over America: tyranny at home." *The Rutherford Institute*, June 28, 2010. Accessed June 4, 2013. Available at: https://www.rutherford.org/publications_resources/john_whiteheads_commentary/drones_over_america_tyranny_at_home.

[20] Declan McCullagh. (2006). "Drone aircraft may prowl U.S. skies," *CNET News*, March 29, 2006. Accessed June 4, 2013. Available at: http://news.cnet.com/2100-11746_3-6055658.html.

[21] Heather Kelley. (2013). "Drones: The future of disaster response," *CNN,* May 23, 2013. Accessed June 4, 2013. Available at: http://whatsnext.blogs.cnn.com/2013/05/23/drones-the-future-of-disaster-response/

[22] Larisa Epatko. (2013). "How Are Drones Used in the U.S.?" *PBS Newshour*, April 18, 2013. Accessed June 4, 2013. Available at: http://www.pbs.org/newshour/rundown/2013/04/how-are-drones-used-in-us.html

[23] Erik Chait. (2010). "Unmanned Aerial Vehicles for Civilian Use: Violating Rights, Privacy, and Safety?" *The Triple Helix*. Fall 2010.

[24] Dave Gilson. (2010). "Predators vs Aliens: Arizona Wants More Drones," *Mother Jones*, May 26, 2010. Accessed June 4, 2013. Available at: http://www.motherjones.com/mojo/2010/05/predator-drones-UAV-border-arizona.

[25] Jennifer Lynch. (2013). "Drone Loans: Customs and Border Protection Records 500 Predator Flights for Other Agencies," *Electronic Frontier Foundation*, September 27, 2013. Accessed October 5, 2013. Available at: https://www.eff.org/deeplinks/2013/09/500-cbp-drone-flights-other-agencies.

[26] Travis Dunlop. (2009). "We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search," *South Texas Law Review* 51 (73). Pp. 180-1.

support, such as assisting SWAT operations.[27] The relatively low cost of such UAVs - about $50,000 for a vehicle with appropriate capabilities for police work, compared to $1 million or more for a police helicopter - makes them appealing. Martin Jackson of the Airborne Law Enforcement Association recognizes that many departments will procure UAVs once the FAA relaxes restrictions on operating the vehicles.[28]

In Canada, the RCMP's stated goals are to have UAV operations as a "viable project that is available to all sections of the RCMP."[29] An RCMP review of the "operational feasibility [of UAVs] within the Lower Mainland District", suggests a range of applications of UAVs for Canadian authorities. Such applications include:

- Identifying hazardous materials
- Conducting search and rescue
- Taking aerial photos of concealed or shadowed/darkened areas within housing complexes in the service of crime prevention
- Supporting tactical situations and performing reconnaissance before putting officers into potentially harmful situation
- Perching UAVs on top of buildings to observe crowds and for videotaping troops in training
- Observing crowd behaviour, the flow of persons/traffic, and for planning associated with major events
- Examining structural integrity and locating survivors during disaster response operations
- Photographing crime scenes to locate evidence
- Providing reconnaissance of suspected explosive devices prior to disposal
- Assessing fire-related damage (such as the extent of fire spread) as well as determining the origin of fires
- Videotaping training exercises for assessment/feedback purposes

---

[27] Peter Finn. (2011). "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *The Washington Post,* January 23, 2011. Accessed June 3, 2013. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

[28] Martin Jackson, in Peter Finn. (2011). "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *The Washington Post*, January 23, 2011. Accessed June 4, 2013. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html.

[29] Dave Domoney. (2012). "F Div UAV Project: Collision Reconstruction Program Handout Material," RCMP, Presentation.

- Reconnoitering vessels before boarding them as well as for water-based search and rescue operations
- Taking aerial photographs to overlay with scale diagram software to better understand crime scenes
- Assessing environments following chemical, biological, radiological, nuclear, and explosive events, as well as to facilitate subsequent triage and direct responder actions[30]

The RCMP's F Division has been selected to test the practicality of UAVs for the national organization. The Canadian tests began with a collision reconstruction unit, but since those tests, UAVs have been adopted by Major Crimes, Forensic Identification, and Emergency Response Team units.[31] While current applications are largely restricted to post-crime practices, tensions between *proactive* and *post-event* surveillance lurk in debates about acceptable uses of drones in Canada. The tension was manifest at the 2012 Unmanned Systems Canada Conference when the national chair of the RCMP UAV working group stated that UAVs were *not* for "proactive surveillance--gathering info on subjects, crowds or riots", "grow operation searchers", "radar/Lidar", nor are they to be "weaponized"[32]. Despite the chair's statements, the RCMP remains interested in how UAVs could be integrated into its operations. As an example, the RCMP's Integrated Beat Enforcement Teams (IBETs) tested UAVs, though officers noted that the vehicles were "inappropriate for surveillance purposes due to, among other reasons, their short battery/flying times, their conspicuity and better technologies currently in existence".[33]

Currently, the RCMP insists that "police use of UAVs for surveillance purposes is strongly discouraged by all stakeholders" and that operating UAV programs demands that "public support … remain favourable".[34] The national police force has explicitly noted cost recovery as potentially making UAV operations a "viable project that is available to all sections of the RCMP".[35] The result of the dual policy positions related to UAVs – that they should be widely integrated, often for cost reasons, while also not

[30] Dave Jewers. (2010). "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[31] Dave Domoney. (2011). ""F" Division RCMP Business Case," RCMP Report on "Funding for UAV (Unmanned Aerial Vehicle) Program, prepared for "F" Division Executive Committee (DEC), April 24, 2011.
[32] Domoney. Unmanned Systems in Canada, Presentation from "2012 Conference, Ottawa" (2012) Pp. 335
[33] Jewers, Dave. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[34] Jewers, Dave. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[35] Jewers, Dave. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.

adopted because of public perceptions – is revealing of the tension within the RCMP itself over how to best proceed with wider UAV deployment.

Section Three – Ramifications of Aerial Surveillance

UAVs can extend or enhance actors' surveillance capabilities by enabling aerial monitoring at (relatively) low costs. Despite the current hesitancy in Canada to deploy UAVs across a wide range of use cases, a broad business case exists for using the vehicles. Such interest is provoked because sensors linked to UAVs would let authorities "amass data about risk probabilities and then manage populations or eliminate network nodes considered to exceed acceptable risk thresholds . . . drones are forms of surveillance in keeping with the precepts of categorical suspicion and social sorting that define other contemporary surveillance systems."[36] In what follows, we discuss the kinds of monitoring afforded by aerial surveillance and their significance. We then, in the next section, discuss how UAVs might fail in the course of their surveillance activities.

Consultants recognize that UAVs "have a 'niche' in performing the three Ds: dull, dirty, and dangerous work, thereby protecting human pilots from fatigue and various environmental hazard."[37] Moreover, given that some UAVs can operate at heights from 75 meters to kilometers in the air, they often have the advantage of being undetectable "to the person(s) or target(s) being surveilled."[38] In light of the altitudes at which UAVs can operate and their ability to remain airborne for extended periods of time, UAV operators can often gather considerable amounts of information about ground-based subjects. As data is aggregated and marshalled into databases for subsequent processing, analysts can develop increasingly honed definitions for the objects that are sighted by UAV instruments. In effect, phenomena can be "stabilized, constrained, and defined in accordance with these database associations and the programs through which they are ordered."[39] In the process of analyzing monitored objects' rote behaviours, objects, and activities are classified as 'normal'; when deviations from the norm arise, an event occurs to which LEAs might respond. In effect, the process of algorithmic aerial surveillance causes a target of surveillance to be "taken up within the

[36] Tyler Wall and Torin Mohahan. (2011). "Surveillance and violence from afar: The politics of drones and liminal security-scapes," *Theoretical Criminology* 15(3). Pp. 239-254.
[37] Rachel L. Finn and David Wright. (2012). "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law and Security Review* 28. Pp. 186.
[38] Rachel L. Finn and David Wright. (2012). "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law and Security Review* 28. Pp. 187.
[39] Jordan Crandall. (2011). "Ontologies of the Wayward Drone: A Salvage Operation," *CTheory*, Published February 11, 2011. Available at: http://www.ctheory.net/articles.aspx?id=693

arena of attention as an exception because that which surrounds it has been standardized, regularized -- transformed into atmosphere."[40]

In effect, persistent or semi-persistent aerial surveillance enhances the ability to monitor for the 'indicators' of disorder because it empowers authorities to monitor individuals without raising their suspicions. Even the RCMP noted that stealth was a positive attribute in a criteria designed for evaluating and contrasting the merits of various UAV technologies,[41] despite the head of the UAV working group asserting that UAVs were not to be used for surveillance. UAV-collected data helps LEAs identify and establish what constitutes normal on the world below the UAV to try to prevent illegal or disorderly action before it becomes a problem. Consequently, the actual act of abnormality is not all that is searched for: the prospect mass and constant surveillance could preemptively identify disorderly behaviour is tightly linked to LEAs' interests in UAVs.

Monitoring and evaluating movement patterns from the air, especially when conducted over an extended time, can reveal a wealth of information about a person, including their familial, political, professional, religious, and sexual associations, as well as potential health ailments.[42] In addition to the previously mentioned equipment that can be fitted to UAVs, they can be outfitted with 'soft biometric' recognition (which "can recognize and track individuals based on attributes such as height, age, gender, and skin colour"[43]) that let UAV operators evaluate the types of persons that surveilled individuals routinely engage with. Moreover, with data about movement and associated habits in hand, it is computationally possible to map out what constitutes normal behaviour for the individual(s) or 'types' of individuals under surveillance, and thus automate the scrutiny of individuals and groups to raise alerts when deviant or suspicious behaviours are detected. This capacity to understand individuals and groups within a normalized social environment leads to the individuals and groups simultaneously functioning as discrete targets of surveillance *and* elements of the 'atmosphere' with regard to the population they are within. Consequently, surveillance

[40] Jordan Crandall. (2011). "Ontologies of the Wayward Drone: A Salvage Operation," *CTheory*, Published February 11, 2011. Available at: http://www.ctheory.net/articles.aspx?id=693
[41] Dave Domoney. (2012). "F Div UAV Project: Collision Reconstruction Program Handout Material," RCMP, Presentation.
[42] Richard M. Thompson II. (2012). "Dones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," *Congressional Research Service*. Published September 6, 2012. Pp. 9-10.
[43] Richard M. Thompson II. (2012). "Dones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses," *Congressional Research Service*. Published September 6, 2012. Pp. 3-4.

is simultaneously made highly specific to deviants and diffuse because a large body of non-deviant, or innocent, individuals are watched to grade their normalcy/deviancy.

Potential surveillance and privacy issues that are associated with UAVs are predominantly linked to breaking people "down into a series of discrete informational flows which are stabilized and captured according to pre-established classificatory criteria."[44] In light of this way of monitoring populations, it is unclear how much of any given person's 'biographical core' is necessarily captured in the course of monitoring ambient populations, where surveillance predominantly focuses on public actions similar to the way in which a police officer would monitor populations. Regardless of whether a person's biographical core is disturbed, the surveillance is "invasive because, independent of whether data protection principles have been respected, the individual's social actions are removed from the intersubjectivity that ground the identity and enables him or her to enter into social relationships with others."[45]

Focusing on whether persistent surveillance has occurred in a public or private space is often unhelpful in ascertaining whether a legal infringement of a person's privacy has occurred. Specifically, when focusing on the nature of discovered knowledge, attention is given to whether the information relates to 'core' or to 'extraneous' information about a given person. Distinguishing between core and non-core data to gauge the nature of discovered knowledge presumes that the individual is the core site of analysis to detect problematic practices. Problematically, what is 'extraneous' to a specific individual could be 'core' to a community that the individual is (or has been) associated with. So, in cases where aerial surveillance does not focus on identifying an individual specifically, but instead ascertains characteristics of the person's temporary or long-term associational groups, the act of monitoring may not 'violate' any specific individuals' personal dignities. Despite the 'non-violation' of enhanced situational awareness capabilities, UAVs as tools for mass surveillance raise serious concerns for association, speech, and unreasonable intrusion by authorities.

To date, LEAs have officially deployed terrestrial optical sensor-based surveillance systems for *situational awareness* purposes that are related to mass surveillance, and they have specifically *not* been described in policy documents as recording or storing captured data that would reveal any detail about a person's personal activities. This language is meant to defray concerns about surveillance. However, despite this

[44] Kevin D. Haggerty and Richard V. Ericson, "The New Politics of Surveillance and Visibility," in *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2007), 2.

[45] Valerie Steeves, "Reclaiming the Social Value of Privacy," in Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, edited by Ian Kerr, Valerie Steeves, and Carole Lucock (Toronto: Oxford University Press), 206.

diversionary language and its use with privacy regulators, the devices have, in fact, been designed to capture, retain, and prospectively disseminate individuals' personal information.[46] In jurisdictions such as Vancouver, the language of 'situational awareness' has been used as a kind of policy shield: such sensors are described as not involved in surveillance in the documents that privacy commissioners and the public examine, even though the technical apparatus is used in targeted instances of surveillance which captures personally identifiable information.[47] Thus, any attempt to mitigate the privacy or surveillance concerns associated with UAVs in Canada by describing them as purely for 'situational awareness' needs to be critically examined, lest the implications of such 'awareness' be lost in the policy discussions.

[46] Rob Wipond. (2012). Vancouver's closed-circuit TV public-surveillance system guidelines contradict privacy pledge," *Straight.com*, May 2, 2012. Accessed September 24, 2013. http://www.straight.com/news/vancouvers-closed-circuit-tv-public-surveillance-system-guidelines-contradict-privacy-pledge. See also: Adam Molnar. (Forthcoming). [Dissertation].

[47] Sean Hier, and Kevin Walby. (2013). "Policy Mutations, Compliance Myths, and Redeployable Special Event Public Camera Surveillance in Canada," *Sociology*, Vol.0(0): 1-17.

Section Four – Failures and Safety

Though UAVs are portrayed as helpful for enhancing public order and safety, concerns exist regarding instrument operation, sensitivity, and dependability. Disruptions of these instruments, if sufficiently catastrophic, bring into question UAVs' overall efficacy as policing aids. In what follows, we account for how UAV surveillance practices may fail because of sensor processing errors, potential unauthorized interference with UAV systems, and more general safety concerns. Such failures, we discuss later in the report, could affect the development of policies and processes regarding LEAs' use of UAVs in Canada.

To begin, inclement weather can disrupt the basic capabilities of the vehicles' sensors; cloudy conditions and high humidity rates can distort images captured through Electo-Optical sensors and forward infrared radar (FLIR) cameras. While these deficiencies can be mitigated using additional sensors - such as moving target indicators and synthetic aperture radar - such sensors increase the basic cost of UAV operation by both demanding additional equipment and increasing the payload weight.[48] Furthermore, camera systems that are linked to more complicated data processing systems may become sites of failure. As an example, when camera systems are used for biometric analysis, the overall efficacy of the surveillance may be questionable because biometric surveillance technologies regularly have problems identifying or discriminating against 'non-normal' bodies.[49] Variations in norms of eye colour and expected depictions of gender and race all present problems for biometric analysis. Biometric recognition algorithms are so problematic that, in the UK, there have been problems identifying Asian bodies and, in Japan, problems identifying "non-Japanese" bodies. In aggregate, the consequence of routine failures to 'properly' identify individuals has been to make the technical systems seem less valuable.

There is also the challenge that despite failed data intake and processing processes, action may still be taken on the collected and analyzed data. Data capture is limited by the calibre of the sensors; as an example, while military-grade UAVs can use advanced cameras, these cameras can also suffer from limited angles of visibility. As a result, military-quality cameras may experience challenges in establishing useful lines of sight

[48] Chad C. Haddal and Jeremiah Gertler. (2010). "Homeland Security: Unmanned Aerial Vehicles and Border Surveillance," *Congressional Research Service*. Published July 8, 2010. Accessed June 1, 2013. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a524297.pdf

[49] Shoshana Magnet. (2009). "Using Biometrics to Revisualize the Canada-U.S. Border," in Ian Kerr, Valerie Steeves, Carole Lucock (eds). *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Cambridge, Mass.: Oxford University Press.

in the 'urban canyons' of modern cities. As a final complicating difficulty, UAV sensing data that is used for retroactive data mining or analysis must be based on data input rates that provide low false positive rates from the relevant sensors. If the false positive rate is high, which indicates that the sensor routinely miscategorize an object or person, mining attempts might be unsuccessful in subsequent analyses because they will be operating based on faulty data. As a result, the efficacy or value of UAVs might be limited based not just on policy, but on the adequacy of sensing systems for differing LEA tasks.

In addition to the UAV limitations that are associated with sensing failures, the value of the UAV systems could be undermined if unauthorized third parties compromise them. As an example, a third party could intercept video feeds or confuse a given UAV's geo-positioning system. In the case of video interception, unencrypted video feeds from UAVs to their base station(s) could be intercepted and viewed in real-time. Moreover, failure to ensure effective video or other communications encryption can lead to unauthorized third parties accessing information that is being streamed from the UAV to its associated ground station(s). Such monitoring could let individuals evade aerial surveillance and has, in the past, been used to avoid Predator drone surveillance. Significantly, the software to capture these kinds of video feeds can be as inexpensive as $26 (USD).[50]

Moreover, many UAVs depend on Global Positioning Systems (GPS) for tracking and flight purposes. GPS lets operators program UAV flight paths and correlate captured sensing data with specific geographic positions. Where civilian GPS technologies (as opposed to military GPS technologies) are used, the UAVs can be 'spoofed' using off-the-shelf equipment that costs under $1000 (USD). Spoofing involves feeding incorrect GPS data to the UAV, such that a third party can provide new spatial coordinates and effectively 'take over' the vehicle's movement or geo-tagging capabilities. This tactic has been successfully performed against civilian UAVs by American researchers.[51]

GPS jammers can also be used when the intent is not to 'control' the UAV but instead to limit its ability to fly. Such jammers can simply prevent a targeted UAV from

[50] Trevor Timm. (2011). "Drones: A deeply unsettling future," *Aljazeera*. Published December 7, 2011. Accessed June 3, 2013. Available at: http://www.aljazeera.com/indepth/opinion/2011/12/201112774824829807.html. Noah Shachtman and David Axe. (2012). "Most U.S. Drones Openly Broadcast Secret Video Feeds," *Wired*. Published October 29, 2012. Accessed June 3, 2013. Available at: http://www.wired.com/dangerroom/2012/10/hack-proof-drone/.

[51] Lorenzo Franceschi-Bicchiera. (2012). "Drone Hijacking? That's Just the Start of GPS Troubles," *Wired*. Published June 7, 2012. Accessed June 2, 2013, Available at: http://www.wired.com/dangerroom/2012/07/drone-hijacking/all/.

ascertaining where it is physically situated. Given that most smaller-size UAVs (in relation to Predator or other large-size military drones) depend on GPS for locational awareness, the loss of such awareness can lead to crashes or other malfunctions.[52] In effect, UAVs are presently a 'brittle' technology, insofar as there is a wide strip of prospective technical vulnerabilities that is linked to systems integrated with UAVs. Furthermore, it's possible to serve malware to the computers or devices that are responsible for operating the devices, which also limits LEAs' capabilities to control their vehicles.[53] All of these failings can seriously disrupt LEAs' drone usage, though such techniques prospectively violate anti-hacking laws.

In addition to technical failings that are associated with cameras and flight control, UAVs are generally more likely to crash compared to piloted vehicles. In the case of military UAVs, "[b]etween 2003 and 2006, U.S. Air Force researchers concluded that 71 percent of UAV crashes could be attributed to "human error factors" caused by their human pilots on the ground." Moreover, the U.S. Navy lost contact with a UAV flying over Washington DC in 2010 as a result of a "software glitch,"[54] indicating deficiencies in command and control capabilities, deficiencies that could be exploited to compromise the flight status of the vehicle. UAVs have also crashed into the deserts of Texas and Arizona as a result of human error and software glitches. Furthermore, the vehicles tend to suffer from limited battery life; according to one officer, this limitation restricts the potential for UAV technologies in public order surveillance.[55] This battery-based limitation also raises the spectre of UAVs literally falling out of the sky should they run out of power over the course of LEA operations.

Thus far we have focused on how UAVs might be used, the ramifications of such uses, and how UAVs might experience significant failures. We now move to take up the governance of UAVs before offering some recommendations for using UAVs and providing some considerations for other researchers.

---

[52] Trevor Timm and Parker Higgins. (2012). "Pwn the Drones: A Survey of UAV Hacks and Exploits," *Hope Number 9* conference. New York: New York City. July 13-15, 2012.

[53] Noah Shachtman. (2011). "Exclusive: Computer Virus Hits U.S. Drone Fleet," *Wired*. Published July 10, 2011. Accessed June 2, 2013. Available at: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

[54] Erik Chait. (2010). "Unmanned Aerial Vehicles for Civilian Use: Violating Rights, Privacy, and Safety?" *The Triple Helix*. Fall 2010. Pp. 8.

[55] Anonymous Interviewee. (2012). *Personal interview with author.* March 3rd, 2012

Section Five – Policy, Regulation, Law, and Contemporary Governance

Though LEAs in Canada have expressed interest in using UAVs in policing operations, they have been somewhat restrained by technology, expertise, and government policy. In this section, we note what regulations UAV operators must comply with, as well as identify some relevant case law that might orient future discussions concerning the use of UAVs for policing purposes. We then proceed to briefly map and arrange the policy communities that are, or that we expect to be, involved in setting LEA-linked UAV policies in Canada.

Law enforcement groups in Canada are increasingly deploying UAVs to achieve policing objectives. Based on our reviews of official policy documents that we obtained from the RCMP, a broad range of Canadian LEAs are developing drone systems. The RCMP currently operates the most UAV platforms (15) in the country, with an additional 2 in planning or nearing completion. Other organizations have obtained, or are currently applying for, UAV clearances. These other organizations include the Ontario Provincial Police (OPP), Halton Regional Police Services, Regina Police Services, Saskatoon Police Department, and the Vancouver Police Department.[56] While more UAVs are being deployed by Canadian LEAs each year, federal authorities continue to insist that "it is still too early to determine how many UAVs the RCMP may purchase in the future."[57]

At the federal level, Transport Canada (TC) is the primary regulator of UAVs. UAVs are distinguished from "model aircraft," which are unregulated and must weigh less than 35 kilograms, be designed for "recreational purposes", and not designed to "carry persons or other living creatures."[58] This distinction exists, even though authorities may be using the same model of vehicle as civilians do for recreation. Though model aircraft can be, and are, used within urban areas, Transport Canada regulates non-recreational flights in these areas. Specifically, before a private or public actor or

[56] Dave Jewers. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[57] Dave Jewers. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[58] Department of Justice. (2013). "Canadian Aviation Regulations," *Government of Canada*, current to September 4, 2013. Accessed September 24, 2013. http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf. Pp. 21.

agency can deploy a UAV in the urban setting, the actor(s) must first receive a Special Flight Operating Certificate (SFOC).[59]

An applicant must meet a series of requirements before receiving a SFOC. In addition to providing personal and contact information about the applicant and operator of the UAV-based practices, an extensive amount of additional information must be provided. Such information includes the following items:

- Type and purpose of the operation
- Dates, alternate dates, and times of the proposed operation
- Complete description, including all pertinent flight data on the aircraft that will be flown
- Security plan for the area(s) of operation and security plan for the area(s) to be overflown to ensure that no hazard is created to persons or property on the surface
- Emergency contingency plan to deal with any disaster resulting from the operation
- Name, address, telephone and facsimile numbers of the person designated to be responsible for supervision of the operation area (Ground Supervisor), if different from the Operation Manager during the operation
- Detailed plan describing how the operation shall be carried out. The plan shall include a clear, legible presentation of the area to be used during the operation. The presentation may be in the form of a scale diagram, aerial photograph or large-scale topographical chart and must include at least the following information:
    - Altitudes and routes to be used on the approach and departure to and from the area where the operation will be carried out
    - Location and height above ground of all obstacles in the approach and departure path to the areas where the operation will be carried out
    - Exact boundaries of the area where the actual operation will be carried out
    - Altitudes and routes to be used while carrying out the operation

[59] Department of Justice. (2013). "Canadian Aviation Regulations, Division IV – Miscellaneous Special Flight Operations," *Government of Canada*, current to September 4, 2013. Accessed September 24, 2013. http://laws-lois.justice.gc.ca/PDF/SOR-96-433.pdf. Pp. 588-589.

- Any other information that is pertinent to the safe conduct of the operation and requested by the Minister[60]

Using a UAV without a SFOC has had consequences for Canadian authorities. This situation was highlighted when a policing detachment received an immediate "cease and desist" order and temporarily lost its UAV because it was operating the vehicle without proper SFOC authorization.[61] Obviously, receiving a SFOC is critical for LEA-based uses of UAVs.

Our research shows that the RCMP presently lacks an overarching "policy governing the use of UAVs,"[62] despite being the policing organization that uses the largest number of UAVs in Canada. The RCMP has, however, created a National Unmanned Aerial Systems Working Group (NUASWG), which is tasked with developing UAV policy across Canada and is comprised of officials from across RCMP divisions E (British Columbia), K (Alberta), F (Saskatchewan), D (Manitoba), G (Northwest Territories), L (Prince Edward Island), B (Newfoundland and Labrador), CAP (National Capital Region), CIO (Chief Information Officer of the Treasury Board of Canada Secretariat), and RCMP Tech OPS (Technical Operations), and without any other groups' involvement. In the absence of formal RCMP policy, the NUASWG "recommends the limitation of RCMP use of the UAS as an investigative aid within the prescribed Transport Canada parameters," which confines the use of UAVs to "Collision Reconstruction, Major Crime Scenes, Search and Rescue, Hazardous Material scenes and ERT calls for service".[63] Similar guidance was provided in a 2010 RCMP policy report.[64] Currently, the guidelines set forth by TC and adopted by LEAs are fairly conservative, though the RCMP is advocating for using UAVs for additional purposes. In particular, at least since 2012, the RCMP has wanted to use UAVs for traffic enforcement applications and has noted it has worked with TC "to try and do some testing in this area.[65] Transport Canada has yet to approve this application, citing privacy concerns.[66]

In addition to TC's approval, any UAV-based policing practice should require state authorities to conduct a Privacy Impact Assessment (PIA) it they suspect that any given

[60] Department of Justice. (2013). "Canadian Aviation Regulations, Part VI – General Operating and Flight Rules, 623.65(d)," *Government of Canada*, current to September 4, 2013. Accessed September 24, 2013. http://www.tc.gc.ca/eng/civilaviation/regserv/cars/part6-standards-623d2-2450.htm.
[61] Jewers, Dave. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[62] Dave Jewers. "Unmanned Aerial Systems (UAS): Operational Feasibility within the Lower Mainland District", RCMP Policy Report, November 2010.
[63] RCMP. (2012). "Briefing Note to the Director General", September 17, 2012.
[64] RCMP. (2012). "Briefing Note to the Director General", September 17, 2012.
[65] RCMP. (2012). "Briefing Note to the Director General", September 17, 2012.
[66] RCMP. (2012). "Briefing Note to the Director General", September 17, 2012.

UAV operation would raise privacy issues. The PIA process is ultimately meant to accomplish the following:

- Provide an overview of the program, its legal authority, institutions that are involved, and the party principally responsible for the program
- Identify and categorize privacy risks and take into account the type(s) of activity; the kinds of personal information that will be collected, used, or disclosed; the duration of the program or activities; technologies that might enable enhanced identification methods and surveillance; or automated personal information analysis
- Analyze how a given program uses, retains, or discloses personal information
- Trace the flow of personal information throughout the lifespan of the program
- Clarify how the program complies with existing privacy laws concerning the collection, retention, accuracy, use, disclosure, technical/policy safeguards, technology, and privacy issues
- Summarize the analysis and provide recommendations for how to manage any risk that is linked with the program[67]

In addition to completing a PIA to identify any privacy issues and limit risks, Canadian authorities must comply with relevant provincial privacy laws.

Ultimately, beyond TC and federal privacy law, little existing case law directly governs aerial surveillance. To date, though the Supreme Court of Canada has identified privacy as "an essential component of what it means to be free" and established the Privacy Act of Canada as a quasi-constitutional document,[68] arguably *R v Tessling* exists as the most substantive position from the Court regarding aerial surveillance.

In *Tessling,* the Supreme Court "examined the constitutionality of the police conducting warrantless searches of private dwelling houses using infra red technology

[67] Treasury Board of Canada Secretariat. (2010). "Directive on Privacy Impact Assessment," *Government of Canada*. Last updated April 1, 2010. Accessed September 24, 2013. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text#appC.

[68] *R. v. Dyment*. (1988])2 S.C.R. 417 at 427:
"The Privacy Act is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society…The *Official Languages Act* and the *Privacy Act* are closely linked to the values and rights set out in the Constitution, and this explains the quasi-constitutional status that this Court has recognized them as having".

during the course of criminal investigations."[69] The Court ultimately found that the heat escaping the defendant's home was meaningless and did not reveal core biographical details. It was on this basis that the defendant had no reasonable expectation of privacy concerning the heat emanations that freely escaped into public space outside the home. Key to the decision was that the emanations gave no insight into the defendant's private life; thus, so long as the monitoring of external patterns does not disclose anything of a person's biographical core of information or affect the dignity, integrity, and autonomy of the individual, no unwarranted search had occurred.[70] Emergent from *Tessling* has been a generalized analogy: "external patterns of [X] on the external surfaces of [Y] is not information in which a respondent has a reasonable expectation of privacy."[71] This analogy has been seen as intensely problematic because by:

> reducing potentially coercive or restrictive state action to atoms, molecules, bits and bytes escaping from a building, backpack or electrical device, by stripping police investigation entirely of its social context, this reductionist approach makes it practically irresistible to think of the information that is emanating into public space as "meaningless" insofar as it does not, by itself, reveal any core biographical information. The *Tessling* analogy therefore has the potential to substantially diminish the scope of section 8 protection in a manner that can only have the effect of significantly shrinking our reasonable expectations of privacy.[72]

While PIAs may be required before authorities begin a UAV-based program, it is unclear given the court's guidance on *Tessling* whether any particular application of UAVs necessarily intrudes on Canadians' privacy. So long as the vehicles do not intrude beyond external patterns on an external surface (i.e. the surface of a home, instead of flying inside a home), and so long as authorities are engaged in policing-based activities, then privacy laws may not preclude UAV programs.

Law professor Lisa Austin argues that, in general, courts that evaluate the intrusions of any government surveillance program will consider privacy facts, discount factors, and

---

[69] Canadian Civil Liberties Association. (2004). "R. v. Tessling: Police Searches with Infra-red Cameras," *Canadian Civil Liberties Association*. March 24, 2004. Accessed September 24, 2013. http://ccla.org/2004/03/24/r-v-tessling-police-searches-with-infra-red-cameras/.

[70] *R v. Tessling*. (2004). SCC 67 at 55.

[71] I. Kerr, M. Binnie, and C. Aoki. (2008). "Tessling On My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System," *Canadian Journal of Criminology and Criminal Justice* 50(3).

[72] I. Kerr, M. Binnie, and C. Aoki. (2008). "Tessling On My Brain: The Future of Lie Detection and Brain Privacy in the Criminal Justice System," *Canadian Journal of Criminology and Criminal Justice* 50(3).

proportionality factors in ascertaining if LEAs have unduly infringed on Canadian residents' privacy. These factors can be classified in the following groupings:

Privacy Factors

- Where did the search occur?
- Was the information intimate or biographical in nature?

Discount Factors

- Was the subject matter in public view?
- Was the subject matter abandoned?
- Was the information in hands of third parties? If so, was it subject to an obligation of confidentiality?

Proportionality Factors

- Was the police technique intrusive in relation to the privacy interest?
- Was the use of surveillance technology itself objectively unreasonable?[73]

As she proceeds to write, "the two key factors for defining a privacy interest are the idea of "place" and "biographical core." The remaining factors either function to discount the privacy interest defined through these twin ideas, or function to assess whether the means chosen to impinge upon privacy are minimally impairing of the interest."[74] From this, we are left without a necessary or clear direction concerning how courts may evaluate UAV-enabled surveillance when the surveillance potentially infringes upon Charter rights.

In addition to court interpretations, official justifications by Canadian authorities about using UAVs for enhancing situational awareness capabilities, but *not* as an explicit surveillance technology, further complicates the aforementioned privacy, discount, and proportionality factors. Specifically, using UAVs to monitor populations may entail transitory or long-term collection of information that is intimate or biographical in nature, regardless of whether such monitoring is 'just' for situational awareness. The same is true of information that is captured over the course of sensitive public events in public areas, such as political demonstrations in public avenues. Even under the justification of enhanced situational awareness, the use of UAVs for such purposes could still be considered intrusive and therefore objectively unreasonable, but

[73] L. M. Austin. (2012). "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law," *Canadian Journal of Law and Society* 27(3).
[74] L. M. Austin. (2012). "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law," *Canadian Journal of Law and Society* 27(3).

it is possible that the language of 'situational awareness' may shield LEAs from critiques that their practices infringe on Canadian citizens' and residents' reasonable expectations of privacy.

Ultimately, the preceding reveals that the federal government lacks a clear policy on UAVs. It also reveals that courts will likely need to clarify the boundaries of legal LEA-driven UAV surveillance. Until national policies are established or court challenges arise, however, the use of UAVs by Canadian policing bodies will likely continue to be somewhat ad hoc and primarily constrained by the SFOC process and LEAs' interests in avoiding public pushback of UAV-based practices.

The relative ambiguity concerning the full range of UAV-based policing operations has been intensified by the ways in which Canadian LEAs have sought UAV training outside of Canada. Despite the fact of confused Canadian governance of UAVs, Canadian policing bodies have been training on how to use UAVs for policing practices. The Vancouver Police Department (VPD) in particular has been training with UAVs since at least 2011. As part of this training, VPD's Military Liaison Unit (MLU) and emergency response team officials have taken part in a series of joint-training exercises with the US Army, Canadian Forces, Victoria Police Services MLU, Calgary Police Services MLU, the US Washington National Guard, the US Marine Corp, and several other US departments at military training facilities in the Washington State.[75] Canadian LEAs and Canadian Forces are training on how to integrate UAVs into emergency response practices that centre on urban conflict operations. Such operations are characterized by urban military conflicts that have been popularized through asymmetrical warfare in Afghanistan as the "three block war".[76]

Importantly, these American-based training operations have let Canadian LEAs and the Canadian Forces engage in UAV-based training in urban-based operations outside of Canadian federal and provincial jurisdictions. This extra-territorial training means that questions concerning the legality of using UAVs in Canada have largely been skirted so long as domestic authorities are not unilaterally adopting the UAVs or associated practices without meeting SFOC requirements and completing PIAs. Moreover, by training in the US, Canadian authorities have avoided engaging in public consultations about the normative appropriateness of using UAVs for strategic and tactical policing operations. In effect, within the context of extra-territorial training, LEAs are developing training regimens and application repertoires that anticipate future uses of UAVs in Canadian locales, often while engaging with UAV manufacturers to develop

[75] Adam Molnar. (2014). "The Geo-Historical Legacies of Urban Security Governance and the Vancouver 2010 Olympics," *Geographical Journal*.
[76] Adam Molnar. (2014). "The Geo-Historical Legacies of Urban Security Governance and the Vancouver 2010 Olympics," *Geographical Journal*.

'reality based' tests meant to prepare for 'real world' policing scenarios.[77] All of this serves to expand LEAs' capabilities whilst deftly avoiding the challenging work of establishing UAV policies and associated case law in Canada, policies and laws that might intrude on the kinds of operations LEAs could conduct using UAVs.

In aggregate, the Canadian situation is characterized by an unevenly developing policy landscape, with some actors developing policy and UAV-usage capacities in closed or extra-territorial domains. The result is that core debates around the appropriateness of Canadian applications of UAVs, and their future applications, are happening outside of a holistic Canadian governance framework. In what follows, we discuss the current and anticipated policy network for UAVs in Canada, with some attention to how different policy communities might affect UAV policy development in Canada.

The Canadian UAV Policy Network

UAVs have not yet become a topic that has significantly penetrated federal policy debates outside of law enforcement circles, Transport Canada standards and working groups,[78] and, to a lesser extent, Canadian Forces military circles.[79] The result is that a relatively closed policy community has formed to identify, frame, and take up policy issues. Given that this community – especially when driven by the RCMP and other law enforcement organizations – has particular orientations towards UAV-based projects (i.e. ascertaining how UAVs might fit into a public safety and policing framework), it is understandably involved in thinking through how these vehicles might be used as force multipliers or to reduce public expenditures. As a policy community that is principally

[77] Adam Molnar. (2014). "The Geo-Historical Legacies of Urban Security Governance and the Vancouver 2010 Olympics," *Geographical Journal*.

[78] Transport Canada's Civil Aviation Regulatory Committee struck a series of working groups since at least 2011, and these groups have routinely focused on the following:

- [Unmanned Aircraft Systems] have been around for decades and will continue to do so
- As aircraft, UAS must be regulated
- Safety of all is paramount
    - Manned and Unmanned

Transport Canada. (2012). "Unmanned Aircraft System (UAS) Overview," for the Special Purpose CARAC Technical Committee Meeting, June 19-20, 2013. Accessed September 25, 2012. https://paroxysms.ca/tc_drones.pdf.

[79] David Pugliese. (2013). "RCAF says it sets the rules for drone flight over Canada," *Ottawa Citizen*, August 16, 2013. Accessed September 25, 2013. http://www.ottawacitizen.com/technology/RCAF+says+sets+rules+drone+flights+over+Canada/8798974/story.html.

concerned with protecting the public, it is, at best, motivated secondarily to ensure that policing practices do not inappropriately infringe on Canadian residents' privacy.[80]

This group of LEAs is involved in developing a policy capacity around UAVs, by way of developing methods of framing UAVs for policing, by identifying potential missions, and by actively considering what LEAs regard as problems (e.g. 'privacy issues') and, presumably, solutions to such problems. The result of this capacity building is an understanding of the empirical capacities of UAVs, demonstrated in a report conducted by the RCMP about UAV-types and potential uses,[81] as well as a nuanced understanding of how the technology may intersect with LEA applications of UAVs. Emergent from this capacity, should a high-profile crime event that captures the political and media agendas arise, LEAs' existing understanding of UAV capacities could be used to explain how Canada-wide UAV policies might alleviate or obviate a similar, subsequent, event. Accompanying any technical or process explanation of how UAVs might alleviate such an event could be proposed legislative or policy language that, once adopted, would authorize more broad-based use of UAVs for law enforcement purposes.

There has been relatively little public analysis or discussion of UAVs by the non-LEA actors who are commonly involved in privacy-related debates. Evidence suggests that this is beginning to change, however. In 2013, the federal Privacy Commissioner, Jennifer Stoddart, stated that:

> There are relatively few drones. There aren't many of them in Canada, and the Department of Transport has to issue those licences, so their operation is fairly well contained. However, the assistant commissioner, who oversaw that file, may be more up to date on the issue than I am.
>
> Obviously, the danger stems from the fact that these devices have the capacity to easily provide information on the daily activities of all Canadians, not to mention that they are pretty inexpensive to buy and can be used by amateurs. That isn't happening just yet. But our office has to be ahead of the curve on such issues. Imagine you're in your backyard or you're out for a leisurely Sunday drive or stroll, and a drone is monitoring you. We have to think that in the future, someone other than the state may have that ability. Will the state do it? It's

[80] Past instances of broad-based surveillance, such as monitoring citizens' vehicular movements based on license plate recognition, warrantless aerial surveillance using infrared cameras, and the collection and parsing of Canadians' trash have all been regarded as non-invasive practices by Canadian LEAs.
[81] Dave Domoney. (2012). "F Div UAV Project: Collision Reconstruction Program Handout Material," RCMP, Presentation.

> worrisome. When and under what conditions will it happen? We see it happening in other countries. Those are the kinds of questions we need to ask.[82]

In beginning to ask questions, the Office of the Privacy Commissioner of Canada has awarded $50,000 to Queen's University researchers to investigate privacy considerations related to public and private uses of UAVs. These researchers are to propose "a forward-looking list of specific recommendations on related privacy requirements, appropriate use and governance of the development of UAVs in Canada."[83] The Information and Privacy Commissioner of Ontario has also demonstrated a proactive interest in UAVs and how potentially privacy-invasive uses of the vehicles could be moderated by 'Privacy by Design' principles.[84] Further, members of civil society and advocate-academics are increasingly examining the role of UAVs in domestic security and surveillance operations.[85] Despite these developments, it remains unclear which actors that advocate for privacy will emerge as important actors in the Canadian UAV policy network.

The full range of actors who are interested in adopting UAVs constitutes a developing policy network. Specifically, federal authorities and some municipal policing bodies have exhibited, and continue to exhibit, interest in using UAVs for domestic law enforcement purposes. These bodies have constituted a formal community, the NUASWG, to debate and establish policy positions. Based on official policy documents, we understand that only members of the RCMP are formally involved in this committee at this time. Transport Canada has principally focused on the safety considerations of UAVs, with any associated privacy considerations being the responsibility of specific UAV-using government bodies to address. To date, the Canadian privacy commissioners have not publicly raised significant concerns concerning the appropriateness of using UAVs for domestic policing functions, nor have members of civil society campaigned against any particular domestic policing uses of UAVs.[86] The result is that the policy network is principally composed of pro-UAV parties, though this could rapidly change if a significant privacy or safety violation is perceived as having occurred in Canada. Until such a violation, however, the policy landscape

---

[82] Jennifer Stoddart. (2013). "Evidence, Monday 22, 2013," Standing Committee on Access to Information, Privacy and Ethics, 41st Parliament, 1st Session.

[83] Office of the Privacy Commissioner of Canada. (2013). "Project Backgrounders Contributions Program 2013-2014," *Office of the Privacy Commissioner of Canada*, Last modified May 2, 2012. Accessed September 24, 2013. http://www.priv.gc.ca/resource/cp/2013-2014/cp_bg_e.asp.

[84] RCMP. (2012). "Briefing Note to the Director General", September 17, 2012.

[85] Based on interviews between authors and other academics and members of civil society.

[86] To clarify, while policing practices that could be associated with UAVs, such as FLIR surveillance or ambient surveillance of populations, have been targets of civil society critiques these critiques have not substantially attended to how UAVs might be implicated in such surveillance practices.

appears to be significantly occupied and driven by government agencies interested in using UAVs for policing purposes.

Given that the RCMP and other policing bodies are restraining how they use UAVs until they address the privacy issues, it is likely these issues will eventually be taken up in formal policy channels. As noted by the Information and Privacy Commissioner of Ontario, federal government regulators (i.e. Transport Canada) have focused on safety as opposed to privacy,[87] effectively externalizing privacy issues to the government bodies that are interested in adopting UAVs for policing practices. Presumably, this means that, at the very least, Canadian privacy commissioners will begin examining privacy concerns linked to UAVs as government departments complete and request feedback on PIAs (in jurisdictions where they are submitted) concerning the use of UAVs.

Given the relative novelty of UAV-based policing surveillance, policy entrepreneurs may emerge from either LEA or more proactive privacy supportive groups. Such entrepreneurs are characterized as developing policy expertise and subsequently working to develop and press for the adoption of novel policy proposals. Based on research being conducted by civil liberties groups and some academics, entrepreneurs might focus on establishing strong privacy protections, on Charter issues as the core 'guide' for aerial surveillance as opposed to utilitarian discussions of cost and technical efficacy, or prioritize safety from inappropriate third-party intrusion of UAVs as reasons to ground UAVs. LEAs, in contrast, may refer to the organizational rationale of situational awareness in lieu of surveillance, or they may appeal to *Tessling* and related decisions by provincial and federal courts and privacy commissioners to justify monitoring individuals in public spaces for security and policing practices. Privacy, by LEA communities, may be understood as a 'warrants for bedrooms, not parks'.

The extent to which any particular focusing event arises is (largely) unpredictable at this stage. However, should UAV systems be found to be inappropriately, inaccurately, or unjustly used to conduct mass surveillance, and if this information is made available to all parties in the policy network as well as to the public and politicians simultaneously, restrictions on UAV uses may follow. In the absence of a given privacy commissioner possessing sufficient regulatory power over authorities, however, it is likely that such conflicts will be resolved in legislatures, judiciaries, or media. If, on the other hand, a major disturbance occurs and, subsequent to the disturbance, UAVs are identified as able to prevent similar events, then politicians and privacy commissioners

[87] Ann Cavoukian. (2012). "Privacy and Drones: Unmanned Aerial Vehicles," *Information and Privacy Commissioner, Ontario, Canada*. Published August 2012.

may be limited in their ability to restrain the expanded use of UAVs for policing purposes.

To date, however, there have been no such focusing events in the Canadian context that would inspire novel policy entrepreneurs to 'stake out' how UAVs ought to be used. Moreover, we have not identified language or policies that would spur entrepreneurs to advance pro- or anti-UAV policies based on the exaggerated speech of public officials.[88] Though there have been publications issued by Canadian privacy commissioners, the discussions tend to either authorize the technologies or raise hypotheticals of harm and resolution. Though such discussions can constitute a developing policy *capacity* that might be drawn upon in the face of a focusing event, it is (arguably) insufficient to demonstrably shape current policies over how UAVs are used by authorities in Canada. In effect, the Canadian policy network that is taking up UAVs remains nascent and is seemingly dominated by LEAs and Transport Canada, even though there is emerging involvement by Canadian privacy commissioners. Moreover, the network has been highly conservative in its efforts to stake out how UAVs could be used by Canadian authorities, and it shows no sign that the pace of internal discussions or deliberations will accelerate rapidly in the near future.

[88] An example of such speech can be found in turning to the United States, with politicians such as Michael Bloomberg (mayor of New York city) asking: "what's the difference whether the drone is up in the air or on the building? I mean intellectually I have trouble making a distinction…Everybody wants their privacy, but I don't know how you're going to maintain it." Gregory Ferenstein. (2013). "Bloomberg: 'We're Going to Have More Visibility And Less Privacy,' Drones and Surveillance Coming." Techcrunch, March 23, 2013. Accessed June 4, 2013. Available at: http://techcrunch.com/2013/03/23/bloomberg-were-going-to-have-more-visibility-and-less-privacy/.

Section Six – Recommendations and Considerations

This report has evaluated the potential uses of UAVs and the implications of those uses and has provided an overview of relevant policies, laws, and policy actors that may affect how Canadian LEAs can use UAVs. In this final section, we provide a set of recommendations for how UAVs be taken up, and we identify a set of issues for subsequent policy analysts to consider in their own evaluations of UAV practices in Canada.

Safety

As discussed in Section Four, a host of highly divergent safety issues are linked to the use of UAVs. Specifically, the vehicles could have their communications streams intercepted, their GPS co-ordination systems disrupted, or pilot error could lead to higher rates of UAV collisions or crashes compared to manned aircraft. As a result of these potential issues, we offer the following recommendations.

Recommendation One

Communications streams between UAVs and their terrestrial monitoring and communications systems should be sufficiently encrypted to prevent unauthorized third parties from intercepting or otherwise disrupting the flow of instructions and data between the vehicle and ground-based officers.

Recommendation Two

A civilian GPS should not be exclusively relied upon for navigating UAVs, and LEAs should have officers prepared to take control of vehicles that experience GPS failures. Preferably, LEAs will rely on encrypted locational systems instead of unencrypted or easily disrupted civilian communications infrastructures.

Recommendation Three

Extensive UAV pilot training should be undertaken before officers are permitted to command and fly UAVs. Ideally, a two-pilot system would be adopted so a second-in-command could take control of the aircraft if the pilot's actions are likely to lead to the vehicle crashing.

Privacy

To date, authorities in Canada have been restrained in how they have adopted UAVs. Privacy and public relations concerns have been identified as inhibitors of widespread adoption of the vehicles. Transport Canada has been focused predominantly on safely flying UAVs, and Canada's provincial and federal privacy commissioners have been relatively silent on the use of UAVs.

Recommendation Four

The RCMP's NUASWG should actively reach out to members of the federal privacy establishment, as well as academics or appropriate members of Canada's civil liberties groups, and include them in the development of LEA-driven UAV policies.

Recommendation Five

The privacy commissioners of Canada should jointly identify actions they believe would infringe upon Canadians' reasonable expectations of privacy and work with LEAs to ensure that policing uses of UAVs respect the privacy of Canadian citizens and residents.

Recommendation Six

Clear policies should be established concerning the data that is collected by UAV sensors. Such policies clarify the types of data that can be collected, how the data is obtained, the period of time data is retained, reasons for which the data can be provided to third parties, and methods of individuals to learn whether UAVs have captured information about themselves.

Policing

Canadian LEAs have expressed interest in using UAVs to improve upon their service delivery. They have not, however, actively sought feedback from the public on how UAVs should or should not be adopted as a tool to serve the public interest.

Recommendation Seven

Policing bodies in Canada that intend to use UAVs should engage in wholesome consultations with members of the public in order to meet the service and privacy expectations of Canadians prior to applying for SFOCs from Transport Canada.

Recommendation Eight

LEAs should be explicit to the public concerning their intent to trial UAVs, and they should publicly disclose all relevant PIAs to build public confidence in how LEAs are using the vehicles.

Recommendation Nine

Before municipal policing organizations deploy UAVs, consultations with relevant police boards should take place in public. These consultations should consider, at a minimum, the cost, uses, benefits, and potential risks or drawbacks associated with adding UAVs to their municipal resources.

Recommendation Ten

Policing bodies have tended to argue that their monitoring of public populations is not surveillance – and thus deserving robust privacy impact assessments – and is instead situational awareness. LEAs and privacy commissioners should carefully articulate whether LEAs' uses of UAVs meet the definitional requirements of situational awareness and ensure that this term is not being used to evade robust privacy oversight.

Governance

We have noted that the policy network invested in Canadian LEAs' uses of UAVs remains relatively nascent. Our report also identifies how Canadian authorities and members of the Canadian Forces are engaged in advanced UAV training in the United States. The result has arguably been to circumvent the development of public policy and clear regulation concerning Canadian LEAs' uses of UAVs.

Recommendation Eleven

All extraterritorial training efforts should be made public knowledge, and training efforts should be justified in accordance with how Canadian LEAs anticipate using UAVs. It is imperative that LEAs not circumvent the democratic development of public policy and any regulatory issues that surround UAVs by covertly training with UAVs outside of the public eye.

Recommendation Twelve

A formal provincial/federal working committee should be established to develop UAV policies for Canadian LEAs. Such a committee should include members of Canada's policing services, privacy commissioners, Transport Canada, civil society, and relevant members of industry. This committee should establish a set of principles and evaluate what kinds of practices should and should not be adopted by LEAs. The committee

should establish federal and provincial guidelines that clearly identify when, how, and under what conditions LEAs can deploy UAVs appropriately.

Recommendation Thirteen

For the public to understand the benefits and drawbacks associated with Canadian LEAs' use of UAVs, it is imperative that information concerning UAV usage be publicized. Consequently, LEAs should provide yearly reports that account for the types of UAVs that they each use, their individual and aggregate flight times, purposes of flights, types of operations involved in UAV deployments, whether and why collected information was useful for LEA purposes, and cost of operating the UAVs to taxpayers.

Analyst Considerations

This report sheds light on how and why UAVs are being deployed in Canada and the policy landscape surrounding such deployments. There are, however, a number of questions for subsequent analysts to take up.

Consideration One

Given the host of surveillance equipment that can be attached to UAVs, further analysis is needed to evaluate the kinds of equipment that Canadian LEAs can purchase for the UAVs that they buy. With this analysis in hand, a detailed accounting of the specific privacy implications of specific pieces of equipment and UAVs ought to be conducted.

Consideration Two

We raise concerns that existing Canadian privacy jurisprudence may facilitate a range of normatively invasive UAV surveillance. An extended legal analysis that holistically considers both provincial and federal, as well as Common Law more generally, is needed to evaluate the full contours of the law concerning UAV-based surveillance.

Consideration Three

UAVs are regarded as relatively inexpensive to operate compared to manned aircraft. Such perceptions, however, are not clearly based in empirical evidence. As such, analysts could conduct long-term evaluations of whether the full-range of operating, training, and other costs linked to UAVs are indeed lower than those associated with operating manned aircraft, or alternatively, to using some forms of terrestrial operation.

Canadian analyses of UAV deployments, including uses and policy development, remains incredibly limited to isolated federal and provincial policy papers. Authorities have expressed, and are demonstrating, considerable interest in how the vehicles are used to enhance and extend their surveillance capabilities. Not all such uses are

inherently problematic. However, all such uses should ideally receive public assent prior to widespread adoption of UAVs to augment policing and emergency management capabilities. If authorities are to be believed, and UAVs genuinely are as significant to LEAs as Tasers, the public should be far more involved than they currently are in establishing the appropriate uses and boundaries for when and how UAVs are adopted by Canadian policing organizations.

Conclusion

This report has discussed how UAVs can be used in the course of conducting aerial surveillance, the broad implications of such surveillance, and safety and civil-rights considerations linked to such surveillance. It has also identified key regulations, laws, and policies that are implicated with deploying UAVs in Canada for policing purposes, as well identifying the contours of the Canadian policy network that is interested in such deployments.

Throughout, we have noted how UAVs might be used but, quite often, there has been limited public information concerning how Canadian policing bodies are using, or would like to use, the vehicles in the course of their regular operations. Similarly, though we know that Canadian authorities are trying to grapple with setting policy for using UAVs, it is unclear how far along such policy making is, what parties have been unofficially consulted, or whether such policies are all-encompassing or specific to only the currently approved UAV uses.

UAVs offer potentially significant cost-savings for LEAs and, in some cases, could be useful in responding to emergency and non-emergency situations in safe and cost-effective ways. However, the potential for intrusive and massive surveillance is a consistent feature as authorities use the vehicles outside of public debate. To combat these perceptions and to ensure that Canadians are satisfied with the privacy protections built into how LEAs use UAVs, public engagement and outreach is needed.

This report offers a number of recommendations. First, UAVs must be proven safe and fit for law enforcement purposes before being adopted by LEAs. Second, LEAs must be genuinely mindful of the privacy considerations that are linked to UAVs and, as part of this, work proactively with privacy commissioners and interested members of civil society to ensure Canadians are satisfied with the privacy protections built into how UAVs are used. Third, Canadian LEAs should be explicit about how they are currently using or training with UAVs and about the purposes to which they want to use UAVs. Moreover, LEAs should clearly consult with Canadians to ensure their operations resonate with Canadians' own interests in how UAVs are used. Finally, the currently uneven governance framework needs improvement: working parties should be formally set up to integrate discussions across provincial/federal lines of responsibility in order to establish a common, high-quality degree of oversight and regulation of UAVs.

These recommendations are predicated on information gathered at the time of writing, and we recognize there is a great deal more work to take up. As a result, further analyses should investigate the kinds of equipment that can be linked to UAVs and

their respective privacy considerations. Further analyses should also more deeply evaluate jurisprudence that might affect how authorities can use UAVs, and it should engage in an economic calculation to understand the actual, instead of rhetorical, cost-savings of UAVs.

As in the United States, UAVs are likely to be used more and more widely, and more and more of the vehicles will soon be flying in Canadian skies. At the moment, however, policy makers are positioned to guide such uses proactively rather than reactively. Policy makers should clarify appropriate uses of UAVs in a political climate that is free from untoward events, such as major equipment failure, that might distract from the host of privacy and surveillance issues that are implicated in the use of UAV technology. The time for such well-balanced policy making is now, and currently all stakeholders have an opportunity to work to ensure that Canadians' safety and privacy are protected while ensuring that the uses of UAVs operate under a robust and comprehensive UAV governance framework.

Appendix A – Acronyms

The following acronyms are used in this report.

Acronym	Spelled-Out Term
ATIP	Access to Information and Privacy
CIO	Chief Information Officer
DEA	Drug Enforcement Agency
DND	Department of National Defence
ERT	Emergency Response Team
FAA	Federal Aviation Authority
FBI	Federal Bureau of Investigation
FLIR	Forward Infrared Radar
GPS	Global Positioning System
IBET	Integrated Beat Enforcement Team
LADAR	Laser Radar
LEA	Law Enforcement Authority
MLU	Military Liaison Unit
NUASWG	National Unmanned Aerial Systems Working Group
OPP	Ontario Provincial Police
PIA	Privacy Impact Assessment
RCMP	Royal Canadian Mounted Police
SFOC	Special Flight Operating Certificate
SWAT	Special Weapons and Tactics
TC	Transport Canada
Tech Ops	Technical Operations
UAS	Unmanned Aerial Systems
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
US	United States
VPD	Vancouver Police Department

About the Authors

This report was researched and written by Christopher Parsons and Adam Molnar. They are the principals of Block G Privacy and Security Consulting.

Christopher Parsons is a Privacy by Design ambassador. He has over a decade's experience working with challenging privacy issues that are linked to digital technologies. He specializes in how Canadian privacy law intersects with digital systems, and the implications of such law on the development and deployment of novel projects and practices. Christopher completed his PhD in the Department of Political Science at the University of Victoria, where he was a fellow at the Centre for Global Studies. Currently, he is a Post-doctoral Fellow at the Citizen Lab at the Munk School for Global Affairs. He has published in the Canadian Journal of Law and Society, European Journal of Law and Technology, Canadian Privacy Law Review, CTheory, book chapters in a series of academic and popular books, and reports.

Adam Molnar has spent over a decade researching, teaching, and consulting on developments in security and privacy, particularly in the areas of policing, national security, and public safety. He specializes in how collaborative governmental initiatives are arranged, and the privacy and security benefits and challenges that follow. Adam is completing his PhD in the Department of Political Science at the University of Victoria, where he was a fellow at the Centre for Global Studies. He is also a Postdoctoral Fellow at the Surveillance Studies Centre at Queen's University. He has published book chapters and policy reports, and he regularly presents his research domestically and internationally.