Privacy and Drones: Unmanned Aerial Vehicles

August 2012

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Information and Privacy Commissioner,
Ontario, Canada

TABLE OF CONTENTS

Foreword

The Panopticon prison design was the creation of English philosopher and social theorist Jeremy Bentham. The design consisted of a circular structure with an "inspection house" at its centre. From this vantage point, managers or guards of the institution were easily able to watch (and control) the behaviour of the inmates stationed around the perimeter. Bentham intended the basic plan to have widespread application.

Bentham's initial concept was later invoked by Michel Foucault (in *Discipline and Punish: The Birth of the Prison*) as a metaphor for modern "disciplinary" societies and their pervasive inclination to observe and normalize. Foucault proposed that not only prisons, but all hierarchical structures (*i.e.*, armies, schools, hospitals, and factories) have evolved through history to resemble Bentham's Panopticon.

Our societies are becoming increasingly acclimatized to panoptic surveillance by closed-circuit television (CCTV) cameras in both public and private spaces, accepting that law enforcement agencies have a legitimate and compelling need to engage in authorized surveillance. However, there is also the potential for serious violations of privacy to arise from the misuse of this technology. Thus we set out video surveillance guidelines to control potential excesses of such technology.[1]

Echoing Bentham and Foucault, the increased use of drones or "unmanned aerial vehicles" has the potential to result in the widespread deployment of panoptic structures that may persist invisibly throughout society.

These developments oblige us to revisit fundamental issues regarding our expectations of privacy. We are called upon to once again fortify our defence of privacy, including respect for activities that occur in public spaces, in order to ensure that this central tenet of freedom remains protected in a manner that is consistent with our shared values. To achieve this end, we must make a commitment to proactively address privacy by embedding privacy into the design of these new technologies. By adopting a *Privacy by Design* (*PbD*) framework to drone technologies, we can address poor privacy practices and outcomes, and prevent the negative impacts that may otherwise be produced. This can enable us to leverage the benefits of these remarkable technologies, while protecting our cherished freedoms and liberty.

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner,
Ontario, Canada

1 Cavoukian, A. (2007). Guidelines for the use of video surveillance in public places. Office of the Information and Privacy Commissioner (Ontario). Online: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=647

Introduction

There has been significant interest in the technology and privacy issues associated with Unmanned Aerial Vehicles (UAVs). This concern is with good reason: in the context of video surveillance, for example, privacy scholars, advocates, and regulators have warned of the dangers of "sleep walking into a surveillance society."[2] In the past, the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian, has promoted both video surveillance guidelines and privacy-protecting technologies.[3]

UAVs present unique challenges, due to their ability to use a variety of sensors to gather information from unique vantage points – often for long periods and on a continuous basis. The prospect of having our every move monitored, and possibly recorded, raises profound civil liberty and privacy concerns. At the same time, there are many desirable benefits associated with these technologies.

The aim of this paper is to provide a background for general privacy readers, as well as for potential users or regulators of UAV activities, as they relate to the collection, use, and disclosure of personal information. The paper is divided into four parts.

In **Part One**, the market for and uses of UAV technologies are discussed. This discussion will highlight the broad trends that suggest increased domestic use of UAVs. This is due in large part to the fact that the technologies are becoming smaller, cheaper, and increasingly more sophisticated.

Part Two of the paper discusses the privacy concerns associated with the deployment of UAV technology. UAV technologies will raise privacy concerns to the extent that their operation involves collection, retention, use, and disclosure of personal information. Because this technology has the built-in potential to provide pervasive Panopticon-like surveillance, we have to ensure more rigorous proactive privacy regulation and design than might otherwise be the case.

In **Part Three** of this paper, we address these concerns by highlighting how a *Privacy by Design (PbD)* approach can assist in ensuring that the benefits of UAV technology are facilitated, while simultaneously ensuring that the threat to individual privacy is reduced.

Part Four lists conclusions and recommendations to address potential privacy issues that could arise from the use of drones.

2 BBC News. (2006). "Britain is 'surveillance society.' " Online: http://news.bbc.co.uk/2/hi/uk/6108496.stm Comments of UK Information Commissioner Richard Thomas.

3 [3]Cavoukian, A. (2008). Privacy and video surveillance in mass transit systems: A special investigative report. Privacy Investigation Report MC07-68. Online: http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7874

PART ONE

UAVs – Current Technologies, Future Trends

Unmanned Aerial Vehicles (UAVs) have been referred to variously as drones, robot planes, pilotless aircraft, Remotely Piloted Vehicles (RPVs), Remotely Piloted Aircrafts (RPAs), and other terms which describe aircraft that fly under the control of an operator with no person aboard. They are most often called UAVs, and when combined with ground control stations and data links, form unmanned aerial systems (UAS).[4] UAVs vary widely in size and capacity. For example, they may have a wingspan as broad as a Boeing 737 or smaller than a radio-controlled model airplane.[5]

Though often associated with military activity, there is also keen interest in UAVs by domestic law enforcement, the private sector, and amateur enthusiasts. This is largely due to the decreasing cost of UAV technology, and to the fact that UAVs have distinct functional advantages over manned vehicles. The reference standards developed by the UAV international community to classify UAV systems are based on such parameters as flight altitude, endurance, speed, Maximum Take-off Weight (MTOW), size, etc. In this section, the UAV market is first discussed in broad terms and is followed by the specific classes and uses of UAV technology.[6]

The UAV market

UAV technology has been regarded by some industry experts as the most dynamic growth sector of the aerospace industry in this decade. A study by the Teal Group estimated that the world market for UAV research and development and procurement was US $6 billion in 2011. This figure is expected to double in the next 10 years (see chart below and note that this figure does not include unmanned combat aerial vehicles (UCAV).[7]

Market barriers for civil and commercial applications include:

- Incomplete or immature air space regulations that encompass UAV systems
- Liability for civil operations
- No secure non-military frequencies

4 Gertler, J. (2012). Homeland security: unmanned aerial vehicles and border surveillance. Congressional Research Service. Online: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA524297

5 Federal Aviation Association (2012). Unmanned Aircraft Systems (UAS). U.S. Department of Transportation. Online: http://www.faa.gov/about/initiatives/uas/

6 The use of unmanned aerial vehicles for combat purposes (UCAV – unmanned aerial combat vehicles) is not discussed.

7 Zaloga, S. J., *et. al.* World Unmanned Aerial Vehicle Systems Market Profile and Forecast. Teal Group Corporation. Online: http://tealgroup.com/

- Negative consumer perception
- Lack of operator training/safety standards
- Limited payload capacity and space restrictions.[8]

The domestic use of UAVs is nonetheless expected to continually push toward smaller platforms that are more manageable and more affordable. It has been noted that the reduced cost of UAVs has become a significant selling point. This is being enabled by the ongoing process of miniaturization of sensors, controls, data link solutions, and computing elements. A UAV system that includes a ground operating computer can cost less than US $50,000, whereas a police helicopter performing the same function can cost up to US $1 million.[9]

A lack of access to national airspace, as well as lack of suitable UAV standards and practices, are among the reasons cited for the relatively slow emergence of the UAV market in the domestic context. Domestic demand is expected to increase over the next decade, starting with government organizations requiring surveillance systems similar to military UAVs, such as coast guards, border patrol organizations, and similar national security agencies.[10]

The European Commission is developing the relevant draft laws to deploy advanced technologies, which include UAVs to patrol its frontiers. It initiated several projects in 2008, under the auspices of the European Border Surveillance System (EUROSUR), aimed primarily at illegal immigration. It has been suggested that smart border control systems be set up at every border crossing and airport in each of the 27 member states of the European Union, and these systems could include the use of UAVs.[11] These market developments have been closely followed by regulators – notably in Germany: On the recommendation of the Federal Commissioner for Data Protection and Freedom of Information (BfDI), an important passage was added to the *Civil Aviation Act* and to the Regulation on Aviation.

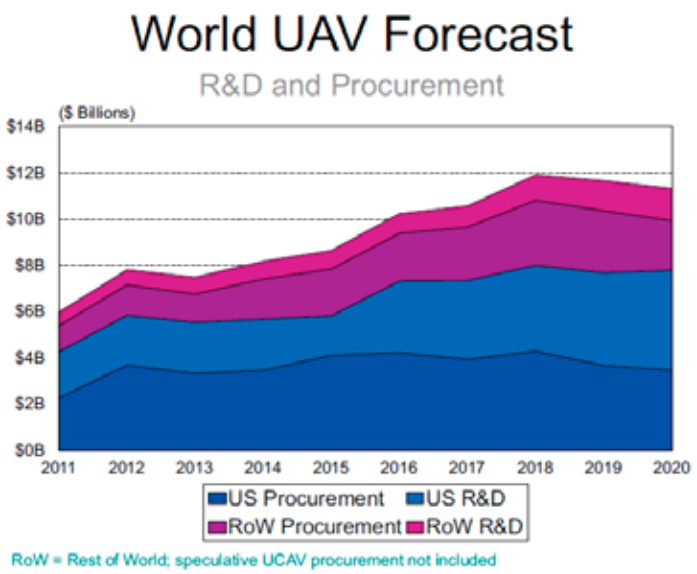
In Germany, the use of UAVs requires authorization by the aeronautical authorities of the Federal States. This authorization may only be granted if the use of UAVs does not violate data protection rights. In order to achieve a consistent practice of granting authorization, the German Ministry of Transport is currently drafting common principles, which will be published in the near future. The BfDI has informed the data protection authorities of the Länder about the new statutory provisions and has raised their awareness of the issue.

8 Rosenberg, A. S. (2009). An evaluation of a UAV guidance system with consumer grade GPS receivers. Ph.D. dissertation, University of Arizona. Online: http://www.casa.arizona.edu/data/abigail/Abigail_Rosenberg_Final_Dissertation.pdf

9 Finn, P. (January 23, 2011). "Domestic use of aerial drones by law enforcement likely to prompt privacy debate." Washington Post. Online: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html

10 *Ibid.*

11 See also related developments in the European Union: Gessat, R. (2012). " 'Smart borders' - Europe's new high-tech frontiers." Deutsche Welle. Online: http://www.dw.de/dw/article/0,,15995226,00.html



Source: World UAV Market Profile and Forecast (Teal Group Corporation)

The market demand for UAV technology is increasing because UAV applications are regarded as effective, low-cost alternatives to manned aircraft. There are more than 220 UAV-related firms in Canada. The sector is also supported by at least 38 postsecondary entities including individual researchers, research centres, and technical training institutes. There are also approximately 60 government organizations with an interest in UAVs.[12]

Systems Overview

The three main features of a UAV system are the:

1. Aircraft with common or other sensor features
2. Ground control station (which may include a data processing centre)
3. Operator (or software instructions).

While the design and performance considerations in UAVs are similar to manned aviation, UAV designers do not have to take an onboard pilot into account. This gives UAVs the advantage of reduced drag and weight (due to the elimination of the cockpit) as well as the ability to sustain a greater amount of g-forces, allowing more complex flight maneuvering.[13] Improvements in navigation and sensor technology have made UAV platforms more reliable in terms of flight control, and

12 Transport Canada (May 3, 2010). Unmanned Air Vehicle (UAV). Government of Canada. Online: http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm

13 Sarris, Z. (2001). Survey of UAV applications in civil markets. Online: http://med.ee.nd.edu/MED9/Papers/Aerial_vehicles/med01-164.pdf

advanced telecommunications technologies permit control at high altitudes over considerable distances.[14]

UAV Classifications

There are three main UAV technologies: micro and mini UAVs, tactical UAVs, and strategic UAVs.[15] These categories, examined below, help us understand the differences in UAV technology. They do not, however, represent classification for the purpose of certification.

Micro and mini UAVs

Micro and mini UAVs are the smallest UAV technology. These platforms fly at low altitudes (below 300 metres). Designs in this category focus on UAVs that can operate in "urban canyons" or inside buildings, flying along hallways, carrying listening and recording devices, transmitters, or miniature TV cameras.[16] Micro UAVs are smaller than mini UAVs, weighing as little as 100 grams; mini UAVs weigh less than 30 kilograms and fly at altitudes between 150 and 300 metres. Micro and mini UAVs are mostly used in civil/commercial applications.

Tactical UAVs

Tactical UAVs are heavier UAVs (from 150 to 1,500 kilograms) that fly at higher altitudes (from 3,000 to 8,000 metres) and are currently used primarily to support military applications. Tactical UAVs can be divided into six subcategories: Close range, short range, medium range, long range, endurance, and Medium Altitude Long Endurance (MALE) UAVs. Long range UAVs use more advanced technology: typically this means a satellite link (or other platform), which acts as a relay in order to overcome the communication problem between the ground station and UAV – a problem caused by the earth's curvature.[17] The lack of satellite communications systems in certain tactical UAVs limits the distances over which close, short, and medium range UAVs can operate. MALE UAVs such as the MQ-1 Predator can operate for more than 40 hours at a maximum range of more than 3,000 kilometres, and can also be equipped to carry and release precision guided missiles.

14 Kumar, R. (1997). Tactical reconnaissance: UAVs versus manned aircraft. Air Command and Staff College, Maxwell Air Force Base, Alabama, U.S.A. Online: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA398405

15 A fourth UAV category is special task UAVs. These are exclusively military technologies and outside the scope of this paper.

16 Bento, M. (2008). Unmanned aerial vehicles: An overview. Inside GNSS 54. Online: http://tinyurl.com/d8wo2kn

17 *Ibid.*

Strategic UAVs

At higher altitudes, UAVs tend to be heavier platforms with longer flight ranges and endurance. The High Altitude Long Endurance (HALE) UAVs are the heaviest UAVs, having Maximum Take-off Weight of up to 12,000 kilograms and a maximum flight altitude of about 20,000 metres. These large platforms can carry larger and heavier payloads and more sophisticated equipment. The military UAV Global Hawk, with 35 hours of endurance, is perhaps the most well-known UAV in this class. An example of a non-military HALE is the electric/solar powered Helios, which is operated by NASA. The Helios uses solar panels to power electrically driven propellers and has set an altitude record of 30,000 metres. The uses of the Helios UAV include observing Earth, mapping, and atmospheric monitoring.

Advanced Surveillance Technologies and UAVs

Most UAVs are (or can be) equipped with camera technologies that can record and transmit photo images to the ground control station. These technologies have become cheaper and more sophisticated and allow image capture at greater distances with greater resolution. It is also possible to equip UAVs with sensors, such as forward-looking infrared (or other thermal imaging) cameras, that can detect infrared radiation, typically emitted from a heat source, and create the "picture" assembled for the video output. Advanced video analytics can apply artificial intelligence to collecting and processing considerable amounts of video data. This, when combined with facial recognition (FR) software, can be used to continuously track individuals while in public and also in private (*e.g.*, through windows or even walls).

Current Status of Domestic Deployment of UAVs in Canada

There has been great interest expressed by Canada's public and private sectors in exploiting the advantages of UAVs. UAVs operate in diverse environments and high risk roles, such as atmospheric research (including weather and atmospheric gas sampling), scientific research, oceanographic research, geophysical research, mineral exploration, imaging spectrometry, telecommunications relay, police surveillance, border patrol and reconnaissance, survey and inspection of remote power lines and pipelines, traffic and accident surveillance, emergency and disaster monitoring, cartography and mapping, search and rescue, agricultural spraying, aerial photography, promotion and advertising, weather reconnaissance, flight research, and fire-fighting monitoring and management.

Transport Canada regulations define a UAV as a power driven aircraft of any size that is operated without a crew on board, for other than recreational purposes. To fly a UAV in Canada, one must obtain a Special Flight Operation Certificate by submitting an application that includes a plan describing how the flight will

be carried out. Safety, rather than privacy, appears to be the focus of the current regulatory regime. UAVs are distinguished from largely unregulated "model aircraft." Model aircraft are small aircraft (35 kilograms or less) used for recreational purposes. Hobbyists with a smartphone can now easily own and operate a camera-enhanced unit. Pictured below is the Parrot AR.Drone Quadricopter,[18] retailing for approximately US $330.

Parrot AR.Drone Quadricopter

Source: Best Buy

The Parrot AR.Drone is a four-rotor quadricopter that can fly indoors or out. The AR.Drone can be controlled using an iPhone, iPod Touch or iPad. The copter generates its own Wi-Fi network, allowing connection to the user's device. The front camera streams all that the copter "sees" directly to the device display.

In 2007, the Kenora Police Service set a precedent when photographs of a scene, taken from a UAV, were admitted as evidence in a trial for the first time.[19] This particular police department used the Draganflyer X6, made by Draganfly Innovations, and the Scout, designed by Aeryon Labs Inc., both Canadian firms. These UAVs are able to take off and land vertically, require less area to operate, and can hover over fixed areas. Manual controls are supplemented by Global Positioning Systems (GPS) and computerized controls that help fly the aircraft.

18 Parrot, A.R. (2012). Frontpage. Online: http://ardrone.parrot.com/parrot-ar-drone/usa/

19 Homeland Security News Wire (February 17, 2011). Canadian police push limits of civilian UAVs laws. Online: http://www.homelandsecuritynewswire.com/canadian-police-push-limits-civilian-uavs-laws

Draganflyer X6

Draganfly Innovations

The remotely-operated miniature helicopter is designed to carry wireless video, still cameras, and light thermal imaging equipment.

Source: Alberto Duadra and Kat Downs, The Washington Post, January 23, 2011

These small UAVs are equipped with several cameras, including digital still, video, and Forward Looking Infrared (FLIR) cameras. Image quality is high, as cameras include vibration dampeners and image stabilization technology. Flights usually last five to 15 minutes and require three ground level operators including a pilot, camera operator, and an aviation safety officer. Radio controlled UAVs such as the Draganflyer X6 are also restricted to line-of-sight flights and maximum altitude of 400 feet, in accordance with Canada's aviation safety laws.

PART TWO

UAVs and Privacy

The uses of UAV (and model aircraft) technologies raise a broad range of issues that relate to collection, retention, use, disclosure, and eventual safe destruction of personal information. The potential for institutional or other abuse, arising as a result of the inappropriate use of these technologies, suggests a need for safeguards tailored to prevent intrusions into privacy and liberty. Whether sensor-enhanced UAVs are used by government agencies, commercial entities, or small personal entities – or whether model aircraft are used by private individuals for recreational purposes – privacy issues must be addressed.

UAVs present unique privacy challenges, due to the manner in which they may collect information. While some of the sensor equipment on board UAVs *may* be commonplace in the consumer electronics marketplace, the ability to gather information dynamically from unique vantage points would appear to distinguish UAV use from other video surveillance cameras, and from data collected using cell phone technology. To determine how we might address the issue, it is worthwhile to consider recent developments, beginning with the U.S. context.

Developments in the United States

The United States has followed an interesting trajectory in the use of surveillance devices and video cameras. In 1986, the U.S. Supreme Court ruled that police use of a private plane deploying video surveillance cameras to detect otherwise hidden marijuana plants in a backyard, did not constitute a search because the observations were made from "public navigable airspace."[20] However, in 2001, in *Kyllo v. United States*,[21] it was held that the use of a thermal imaging device from a public vantage point to monitor the radiation of heat from a person's home constituted a "search" within the meaning of the Constitution and thus required a warrant. The court in *Kyllo* viewed use of thermal imaging equipment (not readily accessible to the public) as being different from observations made in "plain view." The courts' reasoning in these cases centres upon individual expectations of privacy. However individual expectations are likely to change as the technologies of surveillance become more widespread.

More recently, the U.S. Supreme Court, in *United States v. Jones,*[22] considered whether the warrantless use of a tracking device on a motor vehicle operating on public roadways constituted a "search" and therefore violated the protections guaranteed by the Fourth Amendment. On January 23, 2012, the Supreme Court unanimously held that the Government's attachment of the GPS device to the

20 *California v. Ciraolo* 476 U.S. 207 (1986).

21 533 U.S. 27 (2001).

22 564 U.S. ___ (2011). http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf

vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. The decision recognizes that judicial warrants may be constitutionally required to protect privacy interests implicated by the use of sophisticated surveillance technologies, including in public spaces.

In the context of civil aviation, in 2012, the Obama administration signed into law a re-authorization of the Federal Aviation Administration (FAA),[23] requiring that agency to write rules opening U.S. airspace to UAVs. Professors Wittes and Villasenor have suggested that this re-authorization places the FAA at the centre of a set of considerable policy changes, effectively obliging the agency to take on the role of "privacy czar" for UAVs.[24]

In a partial response to the privacy implications of civilian drones operating in US airspace, the Association for Unmanned Vehicle Systems International (AUVSI) issued an Unmanned Aircraft System Operations Industry "Code of Conduct."[25] (The AUVSI is an influential group representing the UAV industry.) Though this is a step in the right direction, the code of conduct is very broad and consists of generic promises not to operate UAVs in a manner that presents "undue risk" and to "respect the privacy of individuals." Critics have noted that there is nothing in the document that attempts to provide a detailed explanation as to how the code will be enforced and by whom.[26]

In Defence of Privacy and Freedom: Privacy Advocates and Civil Society Organizations

The developments in the United States have resulted in concerns being raised by academics and privacy advocates regarding the protection of civil liberties. Stanford Law School researcher Ryan Calo has, for example, remarked that UAV technology represents the "cold technological embodiment of observation."[27] As such, he argues that the issues that these technologies raise among courts, regulators, and the general public may serve as a privacy catalyst, resulting in a backlash that could force us to re-examine the doctrines that allow their use in the first place.

Commenting on U.S. privacy issues in relation to UAVs, University of California, Los Angeles Professor John Villasenor states that the data UAVs acquire can be "correlated with information from mobile devices and smart meters and will become an important component of the growing digital record of nearly everything we do."[28]

---

23 *FAA Modernization Reform Act 2012 H.R.658.*

24 Wittes, B. and Villasenor, J. (April 19, 2012). "Regulating domestic drones on a deadline." The Washington Post. Online: http://tinyurl.com/cs9fx6k

25 AUVSI (2012). Unmanned Aircraft System Operations Industry 'Code of Conduct.' www.auvsi.org/conduct/

26 Vijayan, J. (July 12, 2012). "Drone industry's code of conduct disappoints," Computerworld. Online: http://blogs.computerworld.com/privacy/20685/drone-industrys-code-conduct-disappoints

27 Calo, R. (2011). "The drone as privacy catalyst." 64 Stan. L. Rev. Online 29. http://www.stanfordlawreview.org/online/drone-privacy-catalyst

28 John Villansenor, "High-altitude drones: Coming to a sky near you," Scientific American, February 24, 2012, accessed August 13, 2012, http://tinyurl.com/872otxs

Earlier this year, the FAA requested public comment on unmanned aircraft system test sites. Pursuant to Congressional mandates under the *FAA Modernization Reform Act 2012*, the FAA must "identify six test ranges/sites to integrate unmanned aircraft systems into the national airspace systems."[29] The Washington-based Electronic Privacy Information Center (EPIC) has called for federal agencies to regulate and control the proliferation of UAVs that are used for the purposes of surveillance.[30] More specifically, concerning unmanned aircraft system test sites, EPIC in its submission recommended that the FAA develop evaluation criteria with consideration for the privacy and civil liberties threats arising from drone deployment.[31] EPIC has stated that "because drones possess unparalleled surveillance capabilities, the FAA should assess and prevent privacy risks *before* drones are further deployed."[32] EPIC is particularly concerned with "drone hacking." Drone hacking refers to the process of remotely intercepting and compromising drone operations to pose a threat to the security of lawful drone operations or the process of remotely intercepting and compromising drone operations. To mitigate this problem, EPIC recommends that test sites administered through the FAA should explore (1) the ability to circumvent encryption codes within drone surveillance software and (2) the ability to manipulate hardware to gain access to drone surveillance data.[33]

Washington's Center for Democracy and Technology (CDT) has similarly called for greater approval and oversight processes to be in place in order to protect civil liberties. It has called for the FAA to issue privacy impact assessments, and rules on privacy and transparency, for government and non-government use of UAV technology. CDT believes that, at a minimum, clear processes should be established for law enforcement use of UAVs and for the issuance of UAV licences by the FAA.[34] CDT has commented that in the absence of a baseline consumer privacy law, Congress should consider a targeted approach to privacy, and amend the *FAA Modernization Reform Act* to add civil liberties protections to its approval and oversight process. Such an amendment to the current law would require the Department of Transportation to issue rules for privacy, and the FAA to issue rules for transparency.

In relation to the collection of personal information, CDT recommends that all applications to the FAA for a drone licence include a data collection statement that defines whether the drone will collect information about individuals and, if so, the circumstances under which that information will be retained, used, and disclosed. Using the FIPPs framework, an applicant should describe:

29 FAA Request for comments, Unmanned Aircraft System Test Sites, 77 Fed. Reg. 14319 (proposed Mar. 9, 2012).

30 EPIC (2012) "Unmanned aerial vehicles (UAVs) and drones," Online http://epic.org/privacy/drones/

31 EPIC (2012) Comments of the Electronic Privacy Information Center to the Federal Aviation Administration of the Department of Transportation [Docket No. FAA-2012-0252] Online: http://epic.org/privacy/drones/EPIC-FAA-2012-0252.pdf

32 *Ibid.*

33 *Ibid.*

34 Geiger, H. (2011). The drones are coming. Center for Democracy and Technology. Online: https://www.cdt.org/blogs/Harley-geiger/2112drones-are-coming

1. The purpose for which the drone will be used and the circumstances under which its use will be authorized and by whom
2. The specific kinds of information the drone will collect about individuals
3. The length of time for which the information will be retained
4. The possible impact on individuals' privacy
5. The specific steps the applicant will take to mitigate the impact on individuals' privacy, including protections against unauthorized disclosure
6. The individual responsible for safe and appropriate use of the drone
7. An individual point of contact for citizen complaints.[35]

The American Civil Liberties Union (ACLU) has additionally argued that UAVs raise constitutional issues of a different order to manned aircraft. They have stated that "[b]ecause of their potential for pervasive use in ordinary law enforcement operations and capacity for revealing far more than the naked eye, drones pose a more serious threat to privacy than do manned flights."[36] The ACLU recommends core measures to preserve the privacy Americans have always expected and enjoyed. These include:

- **Usage restrictions.** Drones should not be deployed except:
    - where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon reasonable expectations of privacy, where the government has obtained a warrant based on probable cause; or
    - where there is a geographically confined, time-limited emergency situation in which particular individuals' lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or
    - for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes.
- **Image retention restrictions**. Images of identifiable individuals captured by aerial surveillance technologies should not be retained or shared unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.
- **Public notice.** The policies and procedures for the use of aerial surveillance technologies should be explicit and written, and should be made public. While

35 *Ibid.*

36 Stanley, J. and Crump, C. (2011). Protecting privacy from aerial surveillance: Recommendations for government use of drone aircraft. American Civil Liberties Union. Online: http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies – including the privacy tradeoffs they may entail – are public matters that should be openly discussed.

- **Democratic control.** Deployment and policy decisions about UAVs should be democratically decided based on open information – not made on the fly by police departments simply by virtue of federal grants (or other autonomous purchasing decisions or departmental policy fiats).
- **Auditing and effectiveness tracking.** Investments in UAVs should not be made without a clear, systematic examination of the costs and benefits involved. And if aerial surveillance technology is deployed, independent audits should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can tell generally how – and how often – they are being used, whether the original rationale for their deployment is holding up, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.

Drones' Privacy Challenges: Beyond the Purview of Politics, into the Public Domain

Participants in the UAV deployment/privacy debate were long limited to the "usual suspects:" legislators, industry, regulators, privacy advocates. Only now is the wider public is joining the discussion, prompted at least in part by comments such as these:

> "Drones are a subject on which the far left and the far right can agree. In fact, they do."
>
> *Eugene Robinson, Opinion writer, The Washington Post, August 3, 2012*
> Editorial "Drones? Not over my back yard," referring to the comments below.

> "We need a system of rules to ensure that we can enjoy the benefits of this technology without bringing us a large step closer to a 'surveillance society' in which our every move is monitored, tracked, recorded and scrutinized by the authorities."
>
> *"Protecting Privacy from Aerial Surveillance"*
> Recommendations for Government Use of Drone Aircraft
> A report by the American Civil Liberties Union, December 2011

> "(Drones) flying over our homes, farms, ranches and businesses and spying on us while we conduct our everyday lives is not an example of protecting our rights. It is an example of violating them ... When I have friends over for a barbecue, the government drone is not on the invitation list."
>
> *U.S. Senator Rand Paul* (Republican, Kentucky)
> Opinion/Editorial, CNN, June 14, 2012

In June 2012, identical bills were introduced in the U.S. House of Representatives and Senate: "The Preserving Freedom from Unwarranted Surveillance Act of 2012," "to protect individual privacy against unwarranted governmental intrusion through the use of the unmanned aerial vehicles." In July 2012, a subcommittee of the House of Representatives Committee on Homeland Security, the Subcommittee on Oversight, Investigations and Management, held a hearing "Using Unmanned Aerial Systems within the Homeland: Security Game Changer?" to examine the Department of Homeland Security's role in the domestic use of unmanned aerial systems and determine the extent to which the Department is prepared to ensure oversight of domestic drones. No representative of the DHS testified at the hearing.

PART THREE

Privacy by Design: Preventing "Surveillance by Design"

One approach to ensure privacy is protected is to initially conduct a Privacy Impact Assessment (PIA).[37] A PIA is a process that evaluates privacy implications of information systems. A PIA has three components:

1. A map of the information flows associated with the organization (or the integrated systems, or organization's activity), to determine information decision points and privacy vulnerabilities;

2. A privacy analysis of the information flow, to determine if:

   - privacy principles are adhered to
   - there is technical compliance with statutory and/or regulatory privacy requirements
   - these policies and laws afford the desired privacy protection; and

3. An analysis of privacy issues raised by the system review, including a risk assessment and an evaluation of the options available for mitigating any identified risks.

The process consists of developing an information flow map, applying an appropriately robust set of privacy questions to the information flow, identifying privacy risks, and developing solutions to these privacy risks.

The offices of privacy or data protection commissioners often have PIA templates available to the public. In July 2007, the UK Information Commissioner's Office commissioned a team of researchers to conduct a study into Privacy Impact Assessments (PIAs). The authors found that effective PIAs should do the following:

1. Conduct a prospective identification of privacy issues or risks, before systems and programs are put in place or modified

2. Assess the impacts in terms broader than those of legal compliance

3. Be process (rather than output) oriented

4. Be systematic.[38]

PIAs provide a number of benefits to organizations considering making use of UAVs: They are a means of enhancing informed policy decision-making and

37 Wright, D., & de Hert, P. (2012). Privacy Impact Assessment. Law, Governance and Technology Services, Vol 6.

38 Warren, A., *et. al.* (2008). Privacy Impact Assessments: International experience as a basis for UK Guidance. Computer Law and Security. pp. 233-242.

system design; they anticipate the public's possible privacy concerns; they generate confidence that privacy objectives are being considered. These concerns can be addressed in the development and implementation of single- agency or integrated information systems. The proliferation of UAV technologies and their surveillance capabilities prompts us to prevent the obviously undesirable scenario of "Surveillance by Design."

In addition to conducting a PIA, an important means of achieving proper privacy is through the *Privacy by Design* (*PbD*) approach. *PbD*'s approach is to embed privacy into the design specifications of information technologies, accountable business practices, and networked infrastructures, as the default, right from the outset. It was developed by Commissioner Ann Cavoukian in the 1990s, as a response to the growing threats to privacy that were emerging at that time.

PbD represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches after-the-fact. *PbD* requires an evolution in the way that organizations think about privacy – moving from a reactive mode to a proactive one. Similarly, enshrining *PbD* in regulatory instruments, voluntary codes, and best practices requires an evolution in how policy and law makers approach privacy rule-making.

PbD maps to the well-established Fair Information Practices (FIPs) and modernizes them in two main respects. First, *PbD* principles complement FIPs by ensuring that the protection of privacy is proactive, not reactive; preventative, not remedial. Being proactive about privacy leads to demonstrable methods that recognize poor privacy designs, anticipate poor privacy practices and outcomes, and prevent negative impacts.

Second, *PbD* principles enhance FIPs by accommodating all legitimate interests and objectives in a positive-sum, "win-win" manner. *PbD* avoids the pretence of false dichotomies, such as privacy versus security, demonstrating that it is possible, and far more desirable, to have both. The notion that privacy is the price we must pay for security is exposed for the fallacious argument that it is.

PbD extends to a trilogy of encompassing applications: 1) IT systems, 2) accountable business practices, and 3) physical design and networked infrastructure. Implementing *PbD* means focusing on, and living up to, the following 7 Foundational Principles, which form the essence of *PbD*.

Privacy by Design: 7 *PbD* Principles applied to UAVs

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial.

The *PbD* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events. It does not wait for risks to materialize, nor does it offer remedies for resolving infractions once they have occurred – it aims to prevent them from occurring. In short, *PbD* comes before the fact, not after.

In order to begin protecting privacy in the context of UAV deployment, a necessary first step is to consider the usage limitations associated with these technologies. UAVs should be geographically confined, and operated during specific time periods. The rationale and objectives for implementing the UAV system should be specified, as should the location of equipment, and the personnel authorized to operate the system and to access the equipment. Collection, use, disclosure, and retention of data should be kept to a minimum.

2. Privacy as the ***Default Setting***

We can all be certain of one thing – the default rules! *PbD* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

Recording equipment in UAVs used for video surveillance should be installed in such a way that it monitors only those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings. If cameras are adjustable by operators, this should be restricted, if possible, so that operators cannot adjust, zoom, or manipulate the camera to look at spaces that are not intended to be covered by the video surveillance program. Cameras, infrared sensors, and other remote sensing equipment should be turned on only when necessary, in order to avoid unnecessary "trolling" of data. Organizations should consider overwriting recordings where there is potential for incidental collection of personally identifiable information

Equipment should not monitor the inside of areas where individuals generally have a higher expectation of privacy (*e.g.*, change rooms and public washrooms). The organization should consider restricting video surveillance to time periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.

Any information obtained through the use of UAVs may be used only for the purposes of the stated rationale and objectives set out to protect public safety, and to detect (or deter) and assist in investigating criminal activity. Information should not be retained or used for any other purposes.

3. Privacy ***Embedded*** into Design

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

It is likely that in many instances, UAVs will make use of video recording. If there is a strong possibility of collecting personally identifiable information – especially images of persons or their faces – organizations making use of video recording

equipment should consider the use of anonymous video analytics.[39] Anonymous video analytics software, loaded on the device, processes the video feed to detect whether arrangements of pixels resemble the general pattern of human faces, using such factors as the pixel density and alignment around eyes. These detection algorithms are based on the software having statistically "learned" face patterns, by being trained on an audience database of thousands of face images. The data compiled includes numbers of faces (also known as "impressions"), timing and the duration that faces look, location in the field of view, size of faces, and estimated gender and age bracket. Each video frame is processed to detect the presence of faces, and is then destroyed in real time. The algorithm does not have the capability to recognize individual faces, and there is no database used to match faces, as would be the case with facial recognition technology. A similar approach to embedding privacy into the design of new technology was reported in a special investigation report conducted by the Office of the Information and Privacy Commissioner (Ontario) on privacy and video surveillance in mass transit systems.[40] Here we reported on research at the University of Toronto, described as "Privacy Protected Surveillance Using Secure Visual Object Coding."[41] The process uses cryptographic techniques to secure a private object (personally identifiable information), so that it may be viewed only by designated persons of authority unlocking the encrypted object with a secret key.

4. Full Functionality – ***Positive-Sum***, not Zero-Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum, or doubly enabling "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

It is often argued that it is not possible to have privacy *and* security. Nothing could be further from the truth. By taking into account the legitimate interests of the relevant stakeholders, organizations can take positive steps, such as ensuring that any personally identifiable data is stored securely in a locked receptacle located in a controlled-access area. Each storage device used should be dated and labeled with a unique, sequential number or other verifiable symbol.

Access to storage devices should be restricted to authorized personnel only. Logs should be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Where records are maintained electronically, the logs should also be electronic.

39 Cavoukian, A. (2011). Anonymous video analytics technology and privacy. Online: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1062

40 Cavoukian, A. (2008). Privacy and video surveillance in mass transit systems: A special investigation report." Privacy Investigation Report MC07-68. Online: http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7875

41 See Karl Martin and Konstantinos N. Plataniotis, "Privacy protected surveillance using secure visual object coding," the Edward S. Rogers Sr. Dept. of Electrical and Computer Engineering, University of Toronto, Multimedia Lab Technical Report 2008.01. Online: http://www.dsp.utoronto.ca/projects/surveillance/

5. End-to-End Security – ***Full Lifecycle Protection***

Privacy, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *PbD* ensures cradle-to-grave lifecycle management of information, end to end.

In order to ensure that privacy is protected throughout the data lifecycle, organizations that use UAV technologies should conduct privacy impact assessments (PIA). A PIA is a structured process that assists organizations in reviewing the impact that a new project may have on individual privacy. A PIA also assists government and other public sector organizations to anticipate the public's reaction to any privacy implications of a proposal and as a result, could avert the need for costly program, service, or process redesign. A key goal of the PIA is to effectively communicate those privacy risks that are not addressed through other organizational mechanisms. The PIA is intended to contribute to senior management's ability to make fully informed policy, system design, and procurement decisions.

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***

PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

Consultations should be conducted with relevant stakeholders as to the necessity of the UAV program and its acceptability to the public. This will ensure that the organization's privacy policy and associated industry codes have taken public concerns into account. Organizations should be as open as possible about the UAV program in operation and should make available to the public, upon request, information on the rationale for the program, its objectives, and the policies and procedures that have been put in place. This information may be set out in a pamphlet or leaflet. A description of the program on the organization's website would also be an effective way of disseminating this information. Organizations may also consider the use of push-based notification to concerned individuals who subscribe to this service, indicating when UAVs are in use, via social media such as Facebook or mobile applications.

7. ***Respect*** for User Privacy – Keep it ***User-Centric***

Above all, *PbD* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric – focused on the individual.

The public should be notified, using clearly-written signs prominently displayed where UAVs are being used, in order to provide adequate warning that personal information may be captured. These signs should identify someone who can answer questions about the system, and should include an address, telephone number, or website for contact purposes.

Getting privacy right will be a critical factor in the success of UAV technology. By taking the principled and technology-neutral approach that *PbD* engenders, the process rather than the outcome of technological development can be directed in a manner that protects privacy *and* ensures full functionality.

PbD requires privacy be proactively interwoven into business practices in much the same way as other societal values, such as fairness and transparency. This necessitates establishing privacy at a much deeper level within system design – at the level of code, default settings, and operational systems.

PbD prescribes that privacy be built directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces, and networked infrastructure.[42] The *PbD* approach would ensure protection is embedded from the outset.

PbD principles should be adopted into all aspects of UAV operations in circumstances where personal information may be collected, used, disclosed, retained, transferred, and/or disposed. UAV operators need to ensure that any sort of personal data collection is done with transparency on their part.

Case Study: An environmental consultancy use of UAVs

It is useful to consider how *PbD* would be applied in practice, by a way of a case study. In this case we consider the use of UAVs by an environmental and consultancy firm that provides environmental and social impact assessments and audits, environmental management, planning, and regulatory compliance.

Such a firm routinely uses UAVs to visually inspect locations such as well sites. The well centre is the usual start point for a helicopter UAV. For larger areas, an airplane UAV is normally used. A fixed-wing UAV can have Global Positioning Satellite autopilots that allow them to fly precise tracks over a pre-planned route. Cameras are mounted on the aircraft, typically aimed downward, and snap photos at prescribed intervals.

A mosaic of photos is then "photostitched" together. On the computer, layers can be added onto the graphic, including data collected on the ground and mapped out by handheld GPS. The airplane UAV can be deployed so that others within the company can operate it, essentially by programming in the GPS system.

42 Cavoukian, A. (2010). Privacy by Design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society. Special Issue: Privacy by Design: The Next Generation in the Evolution of Privacy. 3(2), 247-251. Accessed August 13, 2012. doi: 10.1007/s12394-010-0062-y

***Privacy by Design* in Practice:** A company such as this consultancy has many opportunities to apply *PbD* to its operations. As noted earlier, the *PbD* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. *PbD* begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently.

Companies that make use of UAVs need to establish and enforce high standards of privacy – generally higher than the standards set out by global laws and regulation. This requires a privacy commitment that is demonstrably shared throughout the organization. For companies, this would involve ensuring that all employees, particularly ones operating UAV equipment, are aware of the corporate privacy policy, and implement best practices.

By making privacy the default setting, companies that operate UAVs can implement Fair Information Practices (FIPs) into their operations. FIPs highlight the need for purpose specification – the purposes for which personal information is collected, used, retained, and disclosed, shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited, and relevant to the circumstances. Collecting information for the purpose of environmental management in rural areas may not typically involve data subjects. However, where there is potential for collecting personally identifiable information (one could imagine inadvertently recording legitimate activities en route to an inspection site), there will be a need to inform those potentially affected of the possibility of collecting personal identifiable information (PII).

Any PII that is collected needs to be subject to the use limitation principle: the collection of such information is fair, lawful, and limited to that which is necessary for the specified purpose.

Privacy can be embedded into the design and architecture of UAV systems, and used by companies, while enabling core functionality to be delivered. A systemic, principled approach to embedding privacy should be adopted – one that relies upon accepted standards and frameworks which are amenable to external reviews and audits. All fair information practices should be applied with equal rigour, at every step in design and operation. Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and metrics selected.

The full-functionality principle of *PbD* seeks to accommodate all legitimate interests and objectives in a positive-sum, "win-win" manner – not through a dated, zero-sum approach, where unnecessary trade-offs are made. *PbD* avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible (and far more desirable) to have both.

PbD does not involve merely making declarations and commitments – it relates to satisfying *all* of an organization's legitimate objectives, not only its privacy goals. *PbD* is doubly enabling in nature, permitting full functionality – real, practical results and beneficial outcomes, to be achieved for multiple parties.

When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and so that all requirements are optimized to the greatest extent possible. This could be achieved by having the sensitivity and focus of any sensor and recording equipment appropriately calibrated in order to collect the minimum amount of data required.

Privacy is often positioned in a zero-sum manner: as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. *Privacy by Design* rejects taking such an approach – *PbD* embraces legitimate non-privacy objectives and accommodates them in an innovative, positive-sum manner.

All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality. This will involve ensuring that that the pre-planned routes along which UAVs are intended to fly, are assessed for potential privacy violations.

Any PII collected en route should be subject to End-to-End Security – Full Lifecycle Protection. *PbD* ensures cradle-to-grave, secure lifecycle management of information, end to end. Privacy must be continuously protected across the entire domain and throughout the lifecycle of the data in question. There should be no gaps in either protection or accountability. The "Security" principle has special relevance here because, without strong security, there can be no privacy. Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies. Applied security standards must assure the confidentiality, integrity, and availability of personal data throughout its lifecycle including, *inter alia*, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

It will also be important to remain visible and transparent regarding business practices as they relate to privacy. As mentioned earlier, in the *PbD* approach, visibility and transparency are essential to establishing accountability and trust.

Lastly, as in this case study, companies operating UAVs need to keep the interests of potentially affected individuals uppermost, by offering such measures as strong privacy defaults and appropriate notice, and empowering user-friendly options, as mentioned earlier.

The need for strong UAV policy direction in Canada

Whether surveillance-enhanced UAVs are used by government or commercial entities, or model aircraft by private individuals, privacy issues must be addressed. The possibility of near-constant surveillance raises significant concerns related to the chilling effect this is likely to have on public life and individual freedom. As UAVs become more widely used, so too does the potential for widespread deployment of panoptic structures. UAV surveillance that intrudes on private settings and activities will require significant justification.

Canadian Judicial Commentary on Privacy

In *R. v. Dyment*, [1988] 2 S.C.R. 417 at p. 427, Justice La Forest characterized the s. 8 protection of privacy as "[g]rounded in a man's physical and moral autonomy." Privacy, he added, "is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order."

In *R. v. O'Connor*, [1995] 4 S.C.R. 411 at para. 113, Justice L'Heureux-Dubé identified privacy as "an essential component of what it means to be 'free'."

In 2012, in *Jones v. Tsige*, [2012] ONCA 32, the Ontario Court of Appeal drew on the Supreme Court's *Charter* jurisprudence in reaching its conclusion that privacy "has been recognized as a right that is integral to our social and political order," indeed as "worthy of constitutional protection and integral to an individual's relationship with the rest of society and the state."

In the context of law enforcement, the limited jurisprudence dealing with aerial surveillance techniques (such as the use of unsophisticated forward-looking infra-red in drug investigations) does not offer concrete guidance regarding law enforcement's potentially wide use of evolving UAV technologies.[43] To begin, the courts have established judicial principles of reasonableness and proportionality that will be applicable to UAVs.[44] In this context, the more sophisticated surveillance technology becomes, the more likely that it will be capable of intruding on a reasonable expectation of privacy – with the result that its use will require a warrant. In addition, the Supreme Court of Canada has ruled that the tracking of a vehicle on a public roadway raises *Charter* concerns.[45] In advance of a superior court ruling on this point, it is hoped that the policy issues in this area will be debated openly and in a comprehensive manner. Our own view is that, as a general rule, state use of UAVs for the purpose of any sustained surreptitious surveillance should generally require a warrant.

Canadian aviation authorities' regulatory discussions have, to date, focused on safety and improving access to national airspace for UAVs, not on privacy protection.

43 *R v. Tessling,* [2004] SCC 67. http://scc.lexum.org/en/2004/2004scc67/2004scc67.pdf

44 See, for example, the test the court devises in *Tessling* to assess the reasonableness of the accused's expectation of privacy.

45 *R. v. Wise*, [1992] 1 S.C.R. 527 http://scc.lexum.org/en/1992/1992scr1-527/1992scr1-527.html

The collection of personal information by a UAV operator in the course of commercial activity is likely to be regulated under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). In this context, "the organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[46]

The use of model aircraft for recreational purposes does not require a special flight operation certificate. In terms of privacy issues, violations of privacy between individuals are likely to be addressed in Ontario on an *ad hoc* basis by the courts, perhaps under the new tort of intrusion on seclusion.[47]

In the absence of a comprehensive legislative framework, there is a need for a more flexible approach – one that proactively provides strong privacy protection and stimulates innovation in a win-win manner. In short, the subject of UAVs is one that is ripe for the attention of *Privacy by Design*.

46 s. 5(3) *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5)

47 There is no statutory tort of invasion of privacy in Ontario, however, although a common law tort of intrusion upon seclusion has been recognized as a cause of action by the Ontario Court of Appeal. See *Jones v. Tsige,* 2012 ONCA 32.

PART FOUR

Recommendations

The demand for UAVs is set to increase, as UAV technologies are considered in many instances to be effective, low-cost alternatives to manned aircraft. While these developments are remarkable, without careful consideration of their impact on privacy, these technologies may be extremely invasive. There are unique privacy challenges posed, due to UAVs' potential for constant surveillance from vantage points that are difficult to discern. Special use restrictions and regulatory measures will likely be necessary, going forward. The recommendations detailed below highlight some of the main ways that privacy may be protected in this new age of UAVs.

- **Public Debate.** Consultations should be conducted with relevant stakeholders, in instances where UAVs may be used to capture personal information or personally identifiable information (including inadvertently), in order to examine the necessity of any proposed UAV program and if any policies are required to ensure its acceptability to the public.

- **Privacy Impact Assessments.** A PIA can allow for a systematic examination of the impacts and associated benefits involved in deploying UAVs. Before engaging in an activity that involves UAV technology, an assessment should be conducted of the effects that the proposed UAV system may have on personal privacy, and the ways in which any adverse effects can be mitigated, by examining the collection, use, disclosure, and retention of personal information.

- **Transport Regulations.** A privacy policy should be prepared and incorporated into all training and orientation programs of UAV users and service providers. Transport Canada should consider requiring UAV operators seeking a special flight operations certificate to comply with a privacy protection program, naming a responsible privacy officer in the UAV-using organization (or undertaking similar activities that take into account privacy considerations).

- **Usage Restrictions.** Restrictions should be placed on UAV-using organizations as to the extent of personal information they may collect about identifiable individuals. (It should be kept in mind that UAVs may collect such information inadvertently. This is particularly true when UAVs are deployed on a near-constant basis.)

- ***Privacy by Design.*** Rather than taking a privacy compliance approach to system design, organizations should take a proactive *PbD* approach to developing and operating a UAV program which respects privacy. This will ensure that the proposed design and operation of the UAV system limits privacy intrusion, if any, to that which is absolutely necessary to achieve required, lawful goals.

Conclusions

UAVs are likely to become more widely deployed, as there is considerable demand in both the public and private sectors to make use of these technologies. This paper explored the privacy concerns associated with UAV technologies. These concerns may be identified and addressed by undertaking privacy impact assessments in order to ensure the appropriate collection, use, disclosure, and disposal of personal information.

Given the dynamic nature of the technologies of the aerospace industry, adopting a *Privacy by Design (PbD)* approach can help ensure that all legitimate interests and objectives are met in a positive-sum, "win-win" manner. Data collected can be protected while maintaining both the security of the technology and the functionality of the applications. *PbD* can ensure that privacy is embedded at an early stage of development. A *PbD* approach will be fundamental to ensuring privacy is protected in the use of UAVs. Indeed, the future of privacy may well depend on it.

**Information and Privacy Commissioner,
Ontario, Canada**

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

August 2012

Information and
Privacy Commissioner,
Ontario, Canada