Privacy & Drone Surveillance: The Illusive Remedy

Ashley Taborda*

Table of Contents

1. Introduction
2. Defining the Problem: Drones vs. Privacy
   2.1 What is a "Drone"?
      2.1.1 Features and Capabilities
      2.1.2 Drone Applications
         2.1.2.1 Commercial Applications
         2.1.2.2 Recreational Applications
   2.2 The Risks Drones Pose to Privacy
      2.2.1 What is Privacy?
         2.2.1.1 The Development of Privacy as a Concept
         2.2.1.2 An Unsettled Definition
         2.2.1.1 Three Categories of Privacy
            2.2.1.1.1 Informational Privacy: Further Expansion
      2.2.2 Applying the Legal Concept of Privacy to Drones
         2.2.2.1 Inadvertent Data Collection
         2.2.2.2 Data Mining: Facilitating Identification
         2.2.2.3 Degradation of Privacy in the Public Sphere
            2.2.2.3.1 The Reasonableness of Expectations of Privacy in Public
            2.2.2.3.2 The Right to be Anonymous
   2.3 Conclusions on Privacy Risks
3. The Legal Framework
   3.1 Civil Aviation Regulators: Tackling Drone Safety, Ignoring Privacy
      3.1.1 Restricted Drones
      3.1.2 Drones Exempt from the *CARs*
      3.1.1 Model Aircraft
   3.2 Protecting Privacy in a Drone Age
      3.2.1 Privacy Law
      3.2.2 The Common Law
      3.2.3 Property Torts: Trespass & Nuisance
      3.2.4 Actionable Privacy Rights
         3.2.4.1 The Tort of Intrusion Upon Seclusion
   3.3 Conclusions on Protection
4. Conclusion

---

* Ashley Taborda graduated from the JD/MBA program at Western University in 2017 and is currently completing her articles at Osler, Hoskin & Harcourt LLP in Toronto.

1. INTRODUCTION

Despite the infancy of the global drone[1] market, deal values have achieved record-breaking status in recent years, exceeding USD $570 million in 2015 in the commercial sector alone. In 2016, deal values were expected to exceed USD $1 billion, and by 2022, USD $2 billion.[2] Indeed, drones represent today's "most dynamic growth sector of the world aerospace industry."[3] With this growth, coupled with increasingly sophisticated technology, the potential for surveillance will reach its greatest heights; yet, surveillance by the State, or "Big Brother," is no longer the sole concern. As drone use increases, surveillance by corporate and recreational actors, which will be of focus here, will be cause for particular consternation.[4]

The drone, like digital information, the Internet, social media, and heat-detecting cameras, is just another example of a form of technology raising significant privacy concerns.[5] In 2012, in *Jones v. Tsige*,[6] Justice Sharpe of the Ontario Court of Appeal ("ONCA") stated:

> . . . technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter*, has been recognized as a right that is integral to our social and political order.[7]

Despite Justice Sharpe's contention, this threat is not novel. Indeed, in 1890, prompted by privacy concerns associated with the rise of instantaneous photography, Samuel Warren and Louis Brandeis recognized privacy concerns introduced by technology.[8]

---

1 As opposed to commonly used "UAV", or unmanned air vehicle, the term "drone" will be used in this paper, as it is an all-encompassing term referring to any vehicle operating on surfaces or in the air without someone onboard to control it, including model aircraft: Office of the Privacy Commissioner of Canada, "Drones in Canada: Will the Proliferation of domestic drone use in Canada raise new concerns for privacy?," Report by the Research Group of the OPC (Ottawa: OPC, March 2013), online: < https://www.priv.gc.ca > at 2 [OPC — Research Group Report]. See Section 2.1.1, below, for a more comprehensive definition.

2 *DroneII*, "Drone Investment Trends 2016," online: < https://www.droneii.com >; *Grand View Research*, "Commercial Drone Market Worth $2.07 Billion by 2022" (January 2016), online: < www.grandviewresearch.com/press-release > .

3 Office of the Privacy Commissioner of Canada, "Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVS) in Canada," *A Report to the Office of the Privacy Commissioner of Canada, under the 2013-2014 Contributions Program*, by Ciara Bracken-Roche et al. (Ottawa: OPC, 30 April 2014), online: < https://www.priv.gc.ca > at 8 [Bracken-Roche].

4 Graham Mayeda, "My Neighbour's Kid Just Bought a Drone . . . New Paradigms for Privacy Law in Canada" (2015) 35:1 NJCL 59 at 68 [Mayeda].

5 *R. v. Craig*, 2016 BCCA 154, 2016 CarswellBC 918 (B.C. C.A.) at para. 54.

6 2012 ONCA 32, 2012 CarswellOnt 274 (Ont. C.A.) [*Jones*].

7 *Ibid*, at para. 68.

Although the Office of the Privacy Commissioner of Canada (the "OPC") recognizes that new technologies hold "great promise" for Canada's economic growth, it also recognizes the privacy risks that drones represent.[9] As drones become more commonplace, privacy invasions are bound to occur in one form or another. For that reason, those on the other side of the camera must understand their potential avenues for legal recourse. By examining how drones fit into the regulatory landscape, this paper seeks to give light to such avenues, as well as identifying gaps in protection.

To that end, Section 2 will define drones, with a focus on their features and applications. Subsequently, the privacy risks posed by drones will be considered. In Section 3, the legal framework governing drone operation in Canada will be examined. Specifically, drone-specific laws, Canada's private sector privacy legislation, and the common law will be canvassed.

As this paper will illustrate, the Canadian legal system has thus far failed to provide a clear or easily accessible avenue for recourse to those suffering privacy violations as a result of drone surveillance, particularly in public spaces. Beyond statutory deficiencies, the "various guises"[10] by which the common law has protected privacy over the past century have proven inadequate. While the introduction of actionable privacy torts has significantly improved the prospect for recovery, a remedy remains illusory in most scenarios and most provinces. This paper concludes by calling upon the legislature to enhance privacy protection in "the dawn of the age of the drone."[11]

2. DEFINING THE PROBLEM: DRONES VS. PRIVACY

2.1 What is a "Drone"?

2.1.1 Features and Capabilities

Drones, a significant development in robotic technology,[12] refer to any vehicle capable of operating in the air without someone onboard to control it.[13] Drones vary in size, shape, and form, ranging from model aircraft, to mini-

---

8 Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193 at 193 [Warren & Brandeis].

9 OPC — Research Group Report, *supra* note 1 at 1; Office of the Privacy Commissioner of Canada, "Study on the State of Disruptive Technologies: Submission to the House of Commons Standing Committee on Industry, Science and Technology" (Ottawa: OPC, 18 June 2015), online: < https://www.priv.gc.ca > [OPC — Disruptive Technologies].

10 *Jones*, *supra* note 6 at para. 68.

11 Des Butler, "The Dawn of the Age of the Drones: An Australian Privacy Law Perspective" (2014) 37:2 UNSW Law Journal 434 [Butler].

12 Paul D. M. Holden, "Flying Robots and Privacy in Canada" (2016) 14 Can J L & Tech 65 at 65 [Holden].

13 The term "drone" can be further subdivided into (i) "UAV" or unmanned aerial vehicles; (ii) "UAS" or unmanned air systems; (iii) "RPAS" or remote piloted aircraft systems; and (iv) "Model Aircraft." While there are slight differences, the first three terms can

helicopters used by enforcement agencies, to large plane-sized aircraft sent into war zones.[14] As such, drones, which are typically operated by remote operation, can fly at low enough altitudes to trespass, or at high enough altitudes to fly alongside manned aircraft.[15] Due to their flexibility, low cost, and unique capabilities, for many applications, drones represent a desirable alternative to manned flights, which has expanded their use.[16]

As a form of surveillance, drones are persistent, highly targeted, and inexpensive; drones can be deployed on demand, can often stay in the air for longer durations than manned aircraft, and can cover vast and remote areas. Drones are often equipped with advanced technologies including high-power zoom lenses, radar technologies, video analytics, and facial recognition technology.[17] Drones can even be fitted with equipment that impersonates cell phone towers, allowing drones to intercept text messages and record conversations. The United States (''U.S.'') Defense Advanced Research Projects Agency provides an apt example of drone technology. This agency has developed a 1.8 gigapixel video camera for drones, which is capable of tracking sixty-five objects of interest from an altitude of more than 4,500 kilometres. With this camera, nothing can move within a forty square metre radius without being sighted by the camera.[18]

2.1.2 Drone Applications

From Facebook to automobile navigation systems to clinical trials, the applications made possible by the combination of information with computing technology are numerous. Drones, which represent only one example of such technology, have many recognized and potential applications, which are only expected to multiply.[19] Indeed, drones have the potential to benefit public[20] and

---

essentially be used interchangeably, while model aircraft are used exclusively for recreational purposes: OPC — Research Group Report, *supra* note 1 at 2.

14 *Ibid.*

15 Holden, *supra* note 12 at 70; Bracken-Roche, *supra* note 3 at 8.

16 Martin F. Sheehan & Michael Parrish, ''Regulation of Unmanned Aerial Vehicles (''Drones'') in Canada,'' Fasken Martineau LLP, online: < http://www.fasken.com/drones-canada > [Sheehan & Parrish].

17 Facial recognition technology enables drones to recognize and track personal attributes, including height, age, gender, and skin colour: OPC — Research Group Report, *supra* note 1 at 3-4.

18 Matthew L. Burow, ''The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones'' (2013) New Eng J Crim & Civ Confinement 427 at 430 [Burow].

19 OPC — Research Group Report, *supra* note 1 at 12.

20 Although public actors are not the focus here, it should be noted that beyond well-known military purposes, drones are used by the public sector for varied purposes, including intelligence gathering, object targeting, public safety operations, law enforcement, border patrol, emergency services, and commercial aerial imaging: Bracken-Roche, *supra* note 3 at 16.

private actors alike with their diverse aerially-deployed sensor suites and software solutions.[21] For our purposes, commercial and recreational applications will be of focus here.

2.1.2.1 Commercial Applications

Although private sector drone usage is fairly restricted at present, the OPC views drones as an increasingly practical commercial tool.[22] Drones are extremely versatile; drones have been used for activities as varied as navigating the Arctic, delivering pesticides and fertilizers, monitoring the health of crops, monitoring wildlife, and aerial real estate photography.[23] Already, Google and Facebook are contemplating incorporating drone technology into various business applications, including leveraging their networks to communicate Internet and wireless bandwidth signals in parts of the world currently inaccessible by land-based communication networks. Google has also expressed interest in using drone technology's systematic aerial surveillance for its Google Maps initiatives.[24] Amazon, as widely publicized, plans to use drones as delivery vehicles.[25] Thus far, "ambulance drones" have been used to transport defibrillators to heart attack victims and drones have been used to deliver pizza in New Zealand.[26]

The potential applications for drones by corporate actors are seemingly endless.[27] The OPC contemplates drones being used for infrastructure inspection, digital mapping, air quality management and control, and broadcast services.[28] Academics have contemplated the use of drones for the purposes of acquiring evidence for civil and criminal proceedings.[29] However, while drones will clearly facilitate positive outcomes never previously imagined, with their facial recognition software and imaging capabilities, drones can also be used invasively by paparazzi photographers, for stalking, or for industrial espionage.[30]

---

21 Timothy M. Ravich, "Courts in the Drone Age," 42:2 N Ky L Rev 161 at 166 [Ravich].

22 OPC — Research Group Report, *supra* note 1 at 5.

23 Holden, *supra* note 12 at 69.

24 Bracken-Roche, *supra* note 3 at 20.

25 Sheehan & Parrish, *supra* note 16.

26 Kevin Lui, "Watch Domino's Pull Off the World's First Commercial Pizza Delivery by Drone," *Fortune* (16 November 2016), online: <http://www.fortune.com>; Sherry Baxter, "Reasonable Doubt: What you need to know about drones in Canada," *The Georgia Straight* (22 July 2016), online: <http://www.straight.com> [Baxter].

27 Bracken-Roche, *supra* note 3 at 15.

28 OPC — Research Group Report, *supra* note 1 at 5.

29 Ravich, *supra* note 21 at 161.

30 OPC — Research Group Report, *supra* note 1 at 5; Holden, *supra* note 12 at 69.

2.1.2.2 Recreational Applications

In addition to commercial applications, the recreational use of drones by individuals is on the rise. Beyond obvious purposes, such as photography, drones have been used for unexpected activities, such as political activism. In Australia, for example, activists deployed drones to gather video intelligence on an industrial livestock operation.[31] Drones have also been involved in criminal activities, assisting in the smuggling of drugs across borders and of contraband into prisons.[32]

The OPC notes that recreational drones are unique; they are low in cost, highly capable, and no license is required to operate them. To illustrate, the OPC cited the MeCam Flying Copter Camera, which was expected to cost a mere $49 and to come equipped with video recording capabilities, allowing footage to be shared on social media.[33] The Walmart website contains similar examples. The Air Hogs Helix Sentinel Drone, for example, retails for $279.99, offers a high definition 120-degree wide-angle lens camera, 720p Wi-Fi streaming capabilities, a four gigabyte memory card to store footage, and allows for live streaming for up to two smart devices. The Polaroid P300 HD Live Streaming Drone, which retails for $169.98, has a maximum flight height of over one hundred twenty metres, maximum speeds of up to thirty-two kilometres per hour, as well as a high-definition camera that allows for remote adjustment of the camera angle.[34]

While both of the Walmart models above weigh more than 250 grams, and are therefore now regulated by the *CARs*,[35] drones weighing less than 250 grams, which remain unregulated, are also highly capable. Take the racing drone Walkera Rodeo, for example, which is available on Amazon.ca for $285.[36] This drone is equipped with a 600TVL night-vision camera capable of recording with high-definition resolution and has an astounding control range of up to 800 metres.[37] As evidenced by the examples above, recreational drones weighing above and below 250 grams are both highly accessible and well-equipped with advanced technology.

2.2 The Risks Drones Pose to Privacy

As the foregoing section illustrates, drones have numerous capabilities and applications. While drones can certainly be used for positive outcomes, there is nevertheless a risk that drone technology can be used to cause harm. This section

---

31 Bracken-Roche, *supra* note 3 at 17.

32 Baxter, *supra* note 26.

33 OPC — Research Group Report, *supra* note 1 at 5-6.

34 *Walmart*, "Vehicles & Remote Control", online: < www.walmart.ca > .

35 These new regulations will be discussed in detail in Section 3.1.1, below..

36 *Amazon*, "Walkera Rodeo150 Racing Quadcopter DEVO 7 Transmitter 5.8G FPV 600TVL Camera by Walkera," online: < https://www.amazon.ca > .

37 See *Drone Arena*, "Top 10 Camera Drones under 250 Grams" (29 July 2016), online: < www.rcdronearena.com > .

aims to identify the privacy risks posed by drones. To understand drones in that context, however, it is necessary to first understand the legal concept of privacy. To that end, the development of privacy as a concept, privacy's unsettled definition, and the various recognized forms of privacy will be considered here.

2.2.1 What is Privacy?

2.2.1.1 The Development of Privacy as a Concept

In early times, as long as curtains were drawn, no one could see what went on behind castle walls without physically intruding. For that reason, the early roots of privacy law are found in the law of trespass.[38] Warren and Brandeis eloquently described the evolution of privacy rights in their influential essay, "The Right to Privacy." As Warren and Brandeis explained, initially, trespass *vi et armis* protected against physical interference with life or property. Later, upon recognition of the emotional nature of humankind, the law protected against battery and assault. The laws of nuisance and defamation followed, as regard for human emotions extended the scope of "personal immunity" beyond the body to include one's reputation.[39]

Within this context, Warren and Brandeis applauded the common law's ability to adapt:

> . . . thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.[40]

In response to innovations of the time,[41] Warren and Brandeis called for the next stage of common law development: recognition of the right "to be let alone."[42] Within Canadian and American legal scholarship, this right is considered the historical starting point for privacy, although it is important to note that the right to be let alone differs from the concept of "privacy" in certain ways.[43] In some respects, the right to be let alone is broader than privacy, as it demands freedom from interference generally, as opposed to interference with

---

[38] *R. v. Tessling*, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352 (S.C.C.), at para. 15 [*Tessling*].

[39] Warren & Brandeis, *supra* note 8 at 194.

[40] *Ibid* at 195.

[41] These innovations included instantaneous photographs and invasive journalism, and mechanical devices that threatened to "make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'": *ibid.*

[42] *Ibid.*

[43] Notably, since Warren and Brandeis introduced the concept in 1890, it has since developed into four distinct torts in the U.S.: (i) intrusion upon seclusion; (ii) public disclosure of embarrassing facts; (iii) publicity which places the plaintiff in a false light in the public eye; and (iv) appropriation of the plaintiff's name or likeness for the defendant's advantage: William L. Prosser, "Privacy" (1960) 48:3 Cal L Rev 383 at 389.

privacy specifically; at the same time, the right to be let alone is narrower than privacy, as it fails to capture the disclosure of private information.[44]

2.2.1.2 An Unsettled Definition

Although privacy has long been considered worthy of constitutional protection due to its integral relationship to an "individual's relationship with the rest of society and the State,"[45] the importance of privacy appears to be more readily agreed upon than its nature or scope. In *R. v. Dyment*[46], Justice La Forest held that privacy within the context of section 8 of the *Canadian Charter of Rights and Freedoms*[47] is essential to the wellbeing of the individual and has a profound impact on public order. In *R. v. O'Connor*, Justice L'Heureux-Dubé observed that privacy is "an essential component of what it means to be free."[48]

Several decades ago, prominent philosopher Judith Jarvis Thomson asserted that "the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is."[49] Indeed, there are several competing definitions of privacy, many of which differ substantially,[50] although there is widespread agreement that privacy is a dignitary interest, much like reputation.[51] Nevertheless, despite the continuing lack of consensus with respect to what precisely privacy means, and which specific events should be actionable, there appears to be broad agreement that privacy encompasses two broad dimensions: (i) freedom from unwanted intrusion into private affairs and spaces; and (ii) freedom from unwanted disclosure of private information.[52] With the surveillance capabilities of drones, it is the former that is of most concern here.

2.2.1.1 *Three Categories of Privacy*

In *R. v. Spencer*,[53] the Supreme Court of Canada ("SCC") recognized the lack of consensus regarding privacy's nature and limits, noting that privacy is "admittedly a 'broad and somewhat evanescent concept.'"[54] Evanescence

---

44 Holden, *supra* note 12 at 75-76.

45 *Jones*, *supra* note 6 at para 39.

46 1988 CarswellPEI 73, 1988 CarswellPEI 7, [1988] 2 S.C.R. 417 (S.C.C.) at 427 [*Dyment*], as cited in *Jones*, *supra* note 6 at para. 40.

47 Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 [*Charter*].

48 1995 CarswellBC 1098, 1995 CarswellBC 1151, [1995] 4 S.C.R. 411 (S.C.C.) at para. 113, as cited in *Jones*, *supra* note 6 at para. 43.

49 Judith Jarvis Thomson, "The Right to Privacy" (1975) 4:4 Philosophy & Public Affairs 295 at 295, as cited in Chris D. L. Hunt, "The Common Law's Hodgepodge Protection of Privacy" (2015) 66 UNBLJ 161 at 161-162 [Hunt].

50 Holden, *supra* note 12 at 75.

51 Hunt, *supra* note 49 at 172.

52 *Ibid* at 162-163.

53 2014 CarswellSask 342, 2014 CarswellSask 343, 2014 SCC 43 (S.C.C.) [*Spencer*].

54 *Ibid* at para. 35.

notwithstanding, to serve as analytical tools, the SCC recognized three categories of privacy interests, each of which, at least in principle, can be infringed by both intrusions and disclosures.[55] These categories, developed in *Charter* jurisprudence and adopted by the ONCA in *Jones*[56] upon creation of Ontario's new tort of intrusion upon seclusion,[57] are territorial, personal, and informational privacy.[58] According to the SCC, these categories are not mutually-exclusive and often overlap.[59]

Territorial privacy is said to protect the home, as well as other spaces where individuals enjoy a reasonable expectation of privacy. Personal privacy is based on bodily integrity and protects an individual's right not to be touched or to have information disclosed that one wishes to keep concealed. Lastly, informational privacy addresses the "thorny issue of how much information about ourselves and activities we are entitled to shield from the curious eyes of the State."[60]

2.2.1.1.1 Informational Privacy: Further Expansion

To expand upon informational privacy, the SCC cited three further overlapping understandings of informational privacy: secrecy, privacy as control, and privacy as anonymity.[61] While the latter, anonymity, will be considered in greater detail in Section 2.2.2.3.2, the former two understandings will be considered here. The first, secrecy, refers to the retention of private information, such as the expectation of patients that their medical information will be held in confidence by their physicians.[62] In *Jones*, the ONCA cited privacy theorist Alan Westin, who defined privacy as control as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[63] In the *Charter* context, Justice Sopinka asserted that privacy as control is the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[64] This

---

55 Hunt, *supra* note 49 at 163-164.

56 *Jones*, *supra* note 6 at para. 41.

57 Discussed in greater detail in Section 3.2.4.1, below.

58 *Spencer*, *supra* note 53 at para. 35.

59 *Ibid* at para. 35.

60 *Jones*, *supra* note 6 at para. 41; see also *Tessling*, *supra* note 38 at paras. 19-23; *Dyment*, *supra* note 46 at 428-429; *R. v.* ***B. (S.A.)***, 2003 SCC 60, 2003 CarswellAlta 1525, 2003 CarswellAlta 1526 (S.C.C.) at para. 16.

61 *Spencer*, *supra* note 53 at para. 38.

62 See *McInerney v. MacDonald*, 1992 CarswellNB 247, 1992 CarswellNB 63, [1992] 2 S.C.R. 138 (S.C.C.) at 149, as cited in *Spencer*, *ibid* at para. 39.

63 Alan Westin, *Privacy and Freedom* (London: The Bodley Head, 1967) at 7, as cited in *Jones*, *supra* note 6 at 41.

64 *R. v. Plant*, 1993 CarswellAlta 566, 1993 CarswellAlta 94, [1993] 3 S.C.R. 281 at 293, as cited in *Tessling*, *supra* note 38 at para. 26.

"biographical core"[65] includes "intimate details of the lifestyle and personal choices," for example.[66]

2.2.2 Applying the Legal Concept of Privacy to Drones

Despite lacking consensus with respect to privacy's precise definition, it is possible to draw conclusions regarding privacy risks posed by drones using the SCC's analytical tools mentioned above. Of the three categories, drones pose the greatest risk to informational privacy, although territorial and personal privacy can also be affected.

Whether privacy concerns are invoked, and precisely which privacy concerns are invoked, depends largely on the purpose for which drones are used, the context and location of use, and the type of technology employed; these factors affect the extent and type of "personal information"[67] captured.[68] This idea is aptly described in the following comment by the OPC, which developed an interest in drone technology in 2010:

> . . . privacy risks arise from the unique combination of capabilities incorporated into evolving [drone] applications — namely that they couple powerful imaging payloads (high-resolution, infrared, night vision), remote command capability (adding a covert potential) and the ability to linger for periods of time. Where [drones] are in operation, proximity of [the] device to [the] subject and the optimal power of imaging will clearly raise privacy concerns, quite independently of [drones] as a standalone device on their own.[69]

While intentional surveillance is of obvious concern, the inadvertent collection of data by drones is also intensifying concerns about the preservation and protection of individual and collective privacy.[70] Indeed, even drones not used for surveillance collect large amounts of environmental data, which can result in individuals being captured in the background inadvertently.[71]

---

[65] Notably, *Spencer* is argued to have "shrivelled" this conception of the "biographical core," making it only one factor of many to be considered: Chris Hunt & Micah Rankin, "R v. Spencer: Anonymity, the Rule of Law, and the Shrivelling of the Biographical Core" (2015) 61:1 McGill Law Journal 194 at 218 [Hunt & Rankin].

[66] *Tessling*, *supra* note 38 at para. 26.

[67] Using the definition in *Personal Information Protection and Electronic Documents Act*, information is "personal" when there is a possibility of identification, whether alone or in combination with other information: S.C. 2000, c. 5, s. 2(1) [*PIPEDA*]; see also OPC — Disruptive Technologies, *supra* note 9; see also *Gordon v. Canada (Minister of Health)*, 2008 FC 258, 2008 CarswellNat 522, 2008 CarswellNat 6510 (F.C.A.).

[68] OPC — Research Group Report, *supra* note 1 at 12.

[69] Office of the Privacy Commissioner of Canada, "OPC comment to Transport Canada on Unmanned Aerial Vehicles" (Ottawa: OPC, 27 August 2015), online: < https:// www.priv.gc.ca > [OPC - Comment to Transport Canada].

[70] OPC — Research Group Report, *supra* note 1 at 12.

[71] Butler, *supra* note 11 at 434; Holden, *supra* note 12 at 69.

This Section will proceed by first considering the privacy consequences of inadvertent data collection by drones. Subsequently, the use of data mining, which is increasing the amount of personal information captured by drones, will be considered. Finally, the risks that drones pose to privacy in public and to anonymity will be reviewed.

2.2.2.1 *Inadvertent Data Collection*

Justice Posner of the U.S. Court of Appeals for the Seventh Circuit is an advocate for surveillance, at least where surveillance is used to prevent criminal or terrorist assaults. In his view, the deterrence effect, in such cases, outweighs any intrusion.[72] While Justice Posner's contention may be true in the public safety and security context, it is impossible to deny the fact that mass surveillance, whether for public safety initiatives or otherwise, undoubtedly captures large amounts of environmental data, including personally sensitive information.[73] Furthermore, as noted above, even drones not used for surveillance collect large amounts of environmental data. With the rise of big data, the privacy risks associated with data collection, whether inadvertent or otherwise, are not merely a function of the data collected by drones themselves; the risks arise due to the impressive capabilities of data mining.

2.2.2.2 *Data Mining: Facilitating Identification*

Data mining, or data aggregation, involves drawing inferences from matched disparate data sets in order to make predictions about a subject.[74] With aggregated data from multiple sources, including online sources, data mining enables the construction of intimate dossiers of individuals by linking individuals' names with other intimate details, such as social security numbers, preferences, hobbies, family, and friends.[75] Of particular concern, data mining can combine both personal and non-personal information to enable the discovery of information that individuals are unaware that they have revealed and may not wish to reveal, such as predictions by Facebook of a user's sexuality.[76]

Although data collection by the State has been of historical focus, the vast majority of data mining today does not originate with the government. Today's world has been described as a "world of indiscriminate tracking where [commercial enterprises] are stockpiling data about individuals at an unprecedented pace."[77] Clearly, commercial enterprises, including Netflix,

---

[72] Richard A. Posner, "Privacy is Overrated," *NY Daily News* (28 April 2013), online: < http://www.nydailynews.com/opinion > [Posner].

[73] Bracken-Roche, *supra* note 3 at 47-48.

[74] Holden, *supra* note 12 at 80.

[75] Andrew Conte, "Drones with Facial Recognition Technology will end Anonymity, Everywhere," *Business Insider* (27 May 2013), online: < http://www.businessinsider.-com > [Conte].

[76] Holden, *supra* note 12 at 80.

which uses data aggregation to recommend films for customers, and Amazon, which uses data aggregation to manage its supply chain, already see the value of this technique.

Although technology brought data aggregation to the privacy landscape, drones have the potential to amplify the quantity and quality of data collected. Indeed, the OPC has asserted that there is a strong argument that drones will be "surveillance game-changers" due to their attributes, payload technologies, and their ability to collect personal information.[78] With greater volumes of data, facilitated by new types of data and new collection techniques, data mining is further facilitated, allowing for increasingly accurate inferences to be drawn.[79]

By being versatile and persistent, drones also enhance the depth and quality of data collected. Unlike manned aircraft or closed-circuit television,[80] "flying video surveillance threatens to eradicate existing practical limits on aerial monitoring."[81] Sophisticated technology gives drones the physical ability to track an individual's activities and patterns of movement more persistently over time, which has led to drones being referred to as "unblinking eyes in the sky."[82] Drones equipped with surveillance capabilities also have a distinct ability to capture data dynamically from unique vantage points. For example, drones can use thermal imaging devices to capture data through walls with a fine level of detail, or biometric recognition technologies to capture the image of an individual's face from far away.[83]

The National Aeronautics and Space Administration's Global Hawk Mission, which uses drones to track hurricanes, demonstrates the surveillance power of drones. The program's drones can fly up to 17,000 kilometres and stay aloft for up to thirty hours, which allows them to reach and stay in stormy areas that manned aircraft simply cannot. Using an analogy, the mission's director said, "if you drove by a drug dealer's house, you wouldn't catch him; but if you stood there all day, you might."[84] Clearly, the persistent observation facilitated by drones is far more invasive than casual observation.[85]

Although drone technology remains in its infancy, cyber experts believe that very little — mostly research dollars — stands in the way of computers being able

---

77 Julia Angwin, *Dragnet Nation: A Question for Privacy, Security and Freedom in a World of Relentless Surveillance* (New York: Time Books, 2014) at 3, as cited in Holden, *supra* note 12 at 80.

78 OPC — Research Group Report, *supra* note 1 at 10.

79 Holden, *supra* note 12 at 80-81.

80 Closed-circuit televisions are self-contained surveillance systems, typically used by stores and companies: *PC Mag*, "Encyclopedia," online: < www.pcmag.com > .

81 OPC — Research Group Report, *supra* note 1 at 10.

82 *Ibid* at 11.

83 *Ibid* at 11.

84 Brian Handwerk, "5 Surprising Drone Uses (Besides Pizza Delivery)," *National Geographic* (6 June 2013), online: < http://news.nationalgeographic.com > .

85 Holden, *supra* note 12 at 69.

to identify anyone almost instantly.[86] Even if identification is not possible, or if inadvertently captured information does not reach the threshold to be considered part of an individual's "biographical core," it may be "core" to the community with which the individual is associated. Thus, the capture of such data could have a chilling effect on freedoms of association and of speech.[87] For all of the reasons outlined here, it is argued that drones will force the general public to sacrifice both privacy and anonymity,[88] which may have the effect of diminishing expectations of privacy in public.

2.2.2.3 Degradation of Privacy in the Public Sphere

2.2.2.3.1 The Reasonableness of Expectations of Privacy in Public

As "drones with their arrays of sensors take to the sky,"[89] their ability to diminish privacy in public spaces has spurred debate.[90] However, many people question whether expectations of privacy in public are reasonable in the first place. According to dominant theories of privacy, that which is private and undisclosed warrants protection, while that which happens in public does not. According to these theories, privacy is waived by individuals who are out in public.[91] Nevertheless, several scholars disagree, arguing that public and private spheres cannot be so sharply distinguished, as the distinction does not reflect common perceptions of privacy, nor how individuals behave in public.[92] Instead, it is suggested that there are degrees of public and private, depending on what is acceptable in the context.

The OPC supports the latter approach, arguing that there is a reasonable expectation of privacy in public. The OPC argues that while the operation of drones is prohibited in crowded areas for safety reasons, a similar line of reasoning should be employed with respect to privacy. In a 2015 submission to Transport Canada, the OPC stated that "residential areas, schoolyards and shelters, hospitals and prisons, places of worship and memorial sites — all come to mind as spaces which, while perhaps public, carry with them some expectation of privacy when people use [drones]."[93]

In *Spencer*, the SCC agreed, holding that privacy rights are not abandoned the moment someone leaves the privacy of his or her home and enters a public space.[94] In *Spencer*, the SCC quoted *R. v. Wise*, where Justice La Forest stated:

---

[86] Conte, *supra* note 75.

[87] Bracken-Roche, *supra* note 3 at 47.

[88] Conte, *supra* note 75.

[89] Holden, *supra* note 12 at 84.

[90] OPC — Research Group Report, *supra* note 1 at 12.

[91] Holden, *supra* note 12 at 81-82.

[92] *Ibid.*

[93] OPC - Comment to Transport Canada, *supra* note 69.

[94] *Spencer*, *supra* note 53 at para. 44.

> [i]n a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts, we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape.'[95]

In *R. v. Wise*, a driver on public roads was held to have a reasonable expectation of privacy, which was violated by ubiquitous monitoring, even though the vehicle was in public for all to see.[96] In *R. v. Ward,* also cited in *Spencer*, Justice Doherty asserted that:

> personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society.[97]

Clearly, the law appreciates the importance of privacy in public, recognizing that individuals can have a reasonable expectation of privacy in public. As Justice Doherty inferred, anonymity is central to that expectation.

2.2.2.3.2 The Right to be Anonymous

Anonymity, according to the SCC, allows individuals to preserve freedom from identification and surveillance while in public places;[98] in essence, it is the state of being unnamed.[99] In contrast to surveillance, which encourages people to behave differently, anonymity encourages "experimentation" in public places.[100] When an individual goes to the park, drives a car, or walks down the street, movements are not concealed and there is no expectation of confidentiality; an individual does not expect to be identified, or held to rules of behaviour that apply in familiar contexts. Indeed, although someone may expect to be seen in public, that person may expect any observations made about them to vanish into history, rather than remaining on the public record.[101]

As noted above, the SCC in *Spencer* identified "privacy as anonymity" as one of the conceptual understandings of informational privacy. In doing so, Justice Cromwell cited the need for a broadened conception of privacy, which led to the recognition of anonymity as a new dimension of privacy, which the SCC applied specifically to the online context.[102] The SCC emphasized that the

---

95 1992 CarswellOnt 71, 1992 CarswellOnt 1982, [1992] 1 S.C.R. 527 (S.C.C.) at 558, as cited in *Spencer*, *ibid* at para. 44.

96 *Ibid* at para. 43.

97 2012 ONCA 660, 2012 CarswellOnt 12133 (Ont. C.A.) at para. 71, as cited in *Spencer*, *ibid* at para. 48.

98 *Ibid* at para. 43.

99 Burow, *supra* note 18 at 443.

100 Hunt & Rankin, *supra* note 65 at 206.

101 Holden, *supra* note 12 at 83.

102 *Spencer*, *supra* note 53 at para. 41-42; Mayeda, *supra* note 4 at 62-63.

concept was not novel, as anonymity appears in various contexts, such as anonymous surveys and literature.[103] Although the SCC did not recognize a right to anonymity per se, the SCC recognized that there "may be a privacy interest in anonymity, depending on the circumstances."[104]

Although anonymity has positive and negative dimensions,[105] courts, including the SCC in *Spencer*, have recognized the preservation of anonymity as a positive feature of democracy when it promotes debate and discussion on controversial issues.[106] The Internet, for example, facilitates various positive interactions, such as allowing access to advice on deeply personal issues, including anorexia, self-harm, and relationship issues.[107] Anonymity in public can also be a positive feature of democracy. Surveillance drones, for example, are argued to have a chilling effect on the right to peaceful assembly[108] and a proliferation of non-surveillance drones could have a similar effect.

2.3. Conclusions on Privacy Risks

Several factors, each impacted significantly by technology, affect the possible degree of privacy in public spaces. The nature of surveillance is one example, as publicly observable activities dispersed over space and time can be contrasted with systemic observation, which can produce detailed profiles. The permanence or impermanence of observations is also important, with impermanence referring to transient observations made of people in public, which tend to vanish into history. Anonymity, as discussed, is yet another factor.[109]

The privacy challenges posed by drones are not new, at least in kind; indeed, the Internet, digital cameras, and mobile phone tracking present similar risks.[110] However, in degree, privacy risks are amplified by drones. Drones can and will

---

[103] *Spencer*, *ibid* at para. 41-42. Indeed, several novels have been written anonymously, including the classic novel *Nineteen Eighty-Four* by George Orwell. Eric Arthur Blair, a self-conscious man who was deeply afraid of rejection, was the true author of the novel, but anonymity allowed him to remain "namelessly afloat in the sea of a faceless crowd": Burow, *supra* note 18 at 456-457.

[104] *Spencer*, *supra* note 53 at paras. 42, 49.

[105] Just as online anonymity facilitates the exploration of new dimensions of one's identity, it facilitates the distribution of child pornography and creates forums for hate crimes. Anonymity has also contributed to cyberbullying, at least in part, by giving bullies the impression that hurtful messages can be dispersed without consequence: Holden, *supra* note 12 at 79; Senate, Standing Senate Committee on Human Rights, 41st Parliament, 1st Session, *Cyberbullying Hurts: Respect for Rights in the Digital Age* (December 2012) (Chair: Mobina S.B. Jaffer, Co-Chair: Patrick Brazeau), online: < www.parl.gc.ca > at 1, 23 [Jaffer & Brazeau].

[106] See e.g. *King v. Power*, 2015 NLTD(G) 32, 2015 CarswellNfld 62, 364 Nfld. & P.E.I.R. 285 (Nfld. S.C.) at paras. 24-25 [*King*].

[1078] Jaffer & Brazeau, *supra* note 105 at 23.

[108] Bracken-Roche, *supra* note 3 at 31.

[109] Holden, *supra* note 12 at 83.

[110] *Ibid* at 75.

have the effect of diminishing privacy in public by performing systemic observation, by eliminating the impermanence of observations through photographs or video, and by diminishing one's ability to remain anonymous.

3. THE LEGAL FRAMEWORK

As drones become more commonplace, and privacy intrusions by drones increase, members of the public, whether operating drones or living alongside drones, will need to understand both which behaviour offends the law and the potential avenues for redress upon offence. For those that do suffer injury due to privacy invasions by drones, understanding which statutory or common law cause of action, if any, is available is key. Moreover, for the public to feel more comfortable with the idea of drones, an awareness of potential protection is crucial. Therefore, keeping in mind the privacy risks set out in Section 2, this Section seeks to highlight how Canadian laws protect against those risks and where the law falls short.

To that end, to understand the conditions in which drones can and cannot operate, it is first necessary to consider Canada's drone-specific laws. Subsequently, the protection offered by Canada's private sector privacy legislation will be considered. Finally, property and tort law, the traditional common law guardians of privacy, will be canvassed. As will be shown, the current state of the law leaves much to be desired.

3.1 Civil Aviation Regulators: Tackling Drone Safety, Ignoring Privacy

Drone regulation has two licensing streams: Transport Canada, the civil regulatory authority, and the Department of National Defence, which is the military authority.[111] Civil aviation, which is of focus here, is governed by the *Aeronautics Act*[112] and the *Canadian Aviation Regulations*.[113] Additionally, Transport Canada, which is responsible for establishing, managing, and developing safety standards and regulations for civil aviation,[114] has developed specific regulations and guidelines governing the use of drones.[115]

3.1.1 Restricted Drones

Regulations governing "unmanned air vehicles" "("UAVs"),[116] a category of drone, are restrictive and onerous. Although the definition of UAV explicitly

---

[111] OPC — Research Group Report, *supra* note 1 at 6.

[112] R.S.C. 1985, c. A-2. Note that due to the federal government's constitutional power over aeronautics, drones, including model aircraft, are regulated federally: See Sheehan & Parrish, *supra* note 16; see also *Constitution Act*, *1867* (U.K.), 30 & 31 Vict., c. 3, s. 91; *Canada Transportation Act,* S.C. 1996, c. 10.

[113] SOR/96-433 [*CARs*].

[114] OPC — Research Group Report, *supra* note 1 at 6.

[115] Sheehan & Parrish, *supra* note 16; see *CARs*, *supra* note 113, ss. 101.01, 602.41, 603.65-67, 606.02, 623.65.

excludes model aircraft, use is of crucial importance, as model aircraft used for non-recreational purposes, such as for work or research,[117] are considered UAVs.[118] Unless an exemption applies, the *CARs* prohibit the operation of UAVs without a Special Flight Operations Certificate ("SFOC"),[119] which requires the approval of Transport Canada, and restricts the time, space and purposes for which a UAV is permitted to fly.[120] Importantly, penalties for flying a UAV without an SFOC include fines of up to $5,000 for an individual and up to $25,000 for a corporation, while penalties for failing to abide by the terms of an SFOC include fines of up to $3,000 for an individual and up to $15,000 for a corporation.[121]

In assessing SFOC applications, Transport Canada considers all aspects of the application, including the operator's experience, and the nature and complexity of proposed operations. When SFOCs are granted, they are issued for each discrete mission, initially, although longer term SFOCs may be available with a safe operating record. Once authorized, UAV operators must communicate with airspace controllers to coordinate their use of airspace.[122] Despite these restrictions, the number of SFOCs granted per year has increased significantly, from 293 SFOCs between 2007 and 2012, to 1,672 in 2013 alone.[123]

3.1.2 Drones Exempt from the CARs

As restricted drones are subject to intense regulation and scrutiny, unrestricted drones pose a greater risk from a privacy perspective. Unrestricted drones include both exempted UAVs[124] and model aircraft falling outside of the scope of the UAV definition (*i.e.*, recreational drones). With respect to the

---

[116] A UAV "means a power-driven aircraft, *other than a model aircraft*, that is designed to fly without a human operator on board": *CARs*, *supra* note 113, s. 101.01 (emphasis added).

[117] Transport Canada makes it clear that "if you fly a drone for anything other than for the fun of flying," the UAV will be considered as being flown for work or research. Examples of non-recreational activities given include: survey work, agricultural work, inspections, academic research, police work, and aerial photography and videography, including for real estate: Transport Canada, "Applying for a Special Flight Operations Certificate," online: < https://www.tc.gc.ca > .

[118] OPC — Research Group Report, *supra* note 1 at 7.

[119] *CARs*, *supra* note 113, s. 602.41.

[120] Bracken-Roche, *supra* note 3 at 21-22.

[121] Transport Canada, "Flying your Drone Safely and Legally", online: < https://www.tc.gc.ca > .

[122] Sheehan & Parrish, *supra* note 16.

[123] *Ibid.*

[124] Note that model aircraft, operations by autonomous UAVs, and operations by foreign UAV operators are specifically excluded from the scope of the exemption: Transport Canada, Civil Aviation Standards Office, Advisory Circular No. 600-004, "Guidance Material for Operating Unmanned Air Vehicle Systems under an Exemption" (22 December 2016), online: < https://www.tc.gc.ca > at Appendix A [2016 TC Advisory Circular].

former, according to Transport Canada's 2016 Advisory Circular, there are two categories of exempted UAVs: (i) UAVs with a maximum take-off weight of one kilogram or less (previousy two kilograms);[125] and (ii) UAVs with a maximum take-off weight exceeding one kilogram up to and including twenty-five kilograms.[126] The latter category has a maximum speed requirement, and both categories require the UAV to be operated within visual line-of-sight ("VLOS") and are subject to numerous conditions.[127] The existence of such exemptions is significant as in 2014 alone, thousands of exempted UAV operations are estimated to have been conducted; and this number is only expected to grow as UAV technology develops.[128]

Exempted UAV operations are restricted or prohibited in "built-up areas, controlled airspace, aerodromes, forest fire areas, and other restricted locations."[129] The "built-up area" restriction in particular raises an interesting observation. Currently, an exempt UAV is prohibited from operating within three (previously five)[130] nautical miles of a built-up area, which Transport Canada defines as an area with "groups of buildings or dwellings including anything from small hamlets to major cities" and "anything larger than a farmstead."[131] There are further stipulations prohibiting, for example, the operation of UAVs at a lateral distance of less than thirty metres (previously one hundred fifty metres)[132] from any building, structure, vehicle, vessel, animal, or person, unless such operation relates to the subject of the aerial work and only persons inherent in the operation are present.[133]

Notably, it can be inferred from Transport Canada's Advisory Circular that these requirements are entirely safety-related. Firstly, the Advisory Circular suggests that the only reason UAVs cannot be operated near built-up areas is because UAVs are not required to meet technical airworthiness requirements, which increases safety risks to persons and property on the ground.[134] Second, the distances selected fail to prevent privacy invasions; indeed, as we have already seen, drones have the technological capabilities to conduct surveillance from

---

[125] *Ibid*; To review the recent change in weight restrictions, see the 2014 version of the TC Advisory Circular: Transport Canada, Civil Aviation Standards Office, Advisory Circular No. 600-004, "Guidance Material for Operating Unmanned Air Vehicle Systems under an Exemption" (27 November 2014), online: < https://www.tc.gc.ca >, archived at < https://perma.cc/U33W-2KZZ > [2014 TC Advisory Circular].

[126] 2016 TC Advisory Circular, *supra* note 124 at Appendix B.

[127] *Ibid* at Appendices A-B.

[128] Sheehan & Parrish, *supra* note 16.

[129] 2016 TC Advisory Circular, *supra* note 124 at Appendices A-B.

[130] See 2014 TC Advisory Circular, *supra* note 125 at para. 4.2(26).

[131] 2016 TC Advisory Circular, *supra* note 124 at para. 2.3.

[132] See 2014 TC Advisory Circular, *supra* note 125 at para. 4.2(27).

[133] 2016 TC Advisory Circular, *supra* note 124 at para. 4.2(30)

[134] *Ibid*.

distances greater than those prohibited. Interestingly, as highlighted above, Transport Canada has actually decreased these distances with its most recent Advisory Circular, as opposed to increasing them to a level that would better protect the privacy interests of those on the ground.

3.1.1 Model Aircraft

Prior to Transport Canada's *Interim Order No. 8 Respecting the Use of Model Aircraft*,[135] introduced in early 2017, the *CARs* merely prohibited the use of model aircraft in manners hazardous to safety;[136] accordingly, recreational model aircraft weighing under thirty-five kilograms were left essentially unregulated.[137] Clearly, this was concerning in light of the extensive surveillance capabilities of recreational drones, as discussed in Section 2.1.2.2, *supra*. The OPC expressed concern over this gap in regulation, noting that "privacy concerns [were] notably absent in the licensing requirements or regulations established by Transport Canada"[138] and criticizing aviation authorities for excluding model aircraft from the scope of the provisions.[139] As a result of this gap, the *CARs* failed to prevent individuals from employing drones for the purposes of collecting information on public authorities, private sector organizations, or of other individuals by "lateral surveillance."[140] Indeed, without any form of regulation, the recreational use of camera-equipped drones could easily infringe on property, personal, and privacy rights.[141]

In March 2017, the Minister of Transport, the Honourable Marc Garneau, unveiled the aforementioned Interim Order, which took effect immediately and which will remain in effect for up to one year until permanent regulations are put in place.[142] As a result of the Interim Order, model aircraft weighing between 250 grams and thirty-five kilograms[143] are now subject to similar conditions as those mentioned above for exempt UAVs. Specifically, model aircraft cannot be operated at a lateral distance of less than thirty or seventy-five metres (depending on the weight of the model aircraft) from "vehicles, vessels or the public,

---

[135] Transport Canada, "Interim Order No. 8 Respecting the Use of Model Aircraft", Minister of Transport (Ottawa: TC, 16 June 2017), online: <https://www.tc.gc.ca> [Interim Order].

[136] *CARs*, *supra* note 113, s. 602.45.

[137] Model aircraft weighing over thirty-five kilograms, used for any purpose, require a Special Flight Operations Certificate: 2016 TC Advisory Circular, *supra* note 124 at para. 1.3(2).

[138] OPC — Research Group Report, *supra* note 1 at 7.

[139] *Ibid* at 5.

[140] Bracken-Roche, *supra* note 3 at 17.

[141] Baxter, *supra* note 26.

[142] Transport Canada, "Transport Canada Introduces Measures to Protect Canadians from Reckless Drone Use," (Ottawa: TC, 16 March 2017), online: <https://canada.ca/en/transport-canada/news>.

[143] Interim Order, *supra* note 135, s. 3(1).

including spectators, bystanders or any person not assicated with the operation of the aircraft."[144] Furthermore, model aircraft must be operated within VLOS, must be operated at least nine kilometres from any airport, cannot be operated at night, and cannot be operated at an altitude higher than ninety metres.[145] Finally, the Interim Order obliges model aircraft owners to display their name, address, and telephone number on the exterior of the aircraft.[146] Individuals that fail to abide by the new rules may be subject to fines of up to $3,000.[147]

While this Interim Order is a notable improvement over the complete state of non-regulation that existed previously, several models of consumer drones, generally possessing cameras, weigh less than 250 grams; these models remain unregulated, meaning the new regulations cannot effectively "curtail would-be peeping toms."[148] Moreover, much like the SFOC exemptions, the Interim Order is heavily, if not exclusively, focused on safety. This safety focus is demonstrated in the Interim Order's Preamble, which states:

> [w]hereas the annexed *Interim Order No. 8 Respecting the Use of Model Aircraft* is required to deal with a significant risk, direct or indirect, to aviation safety or the safety of the public.[149]

Comments made at the unveiling of the Interim Order by both Garneau and the Chief Superintendent of the Royal Canadian Mounted Police echo the same sentiment.[150]

A further issue that remains post-Interim Order is the challenge of unmasking the anonymous drone operator. Although the Interim Order's new requirement obliging model aircraft owners to display their name, address, and telephone number on the device sought to address this issue, its efficacy is questionable. Indeed, the combination of size and distance will likely make this information unreadable to someone who wishes to report intrusive drone activity. Prior to the Interim Order, the OPC had suggested physical plates, painted numbers or decals, and unique signature signals, such as radio frequency identification devices ("RFID")[151] as potential alternatives.[152] Laura Emmett, a

---

[144] *Ibid*, s. 5(3)-(4).

[145] *Ibid*, s. 5(1)(a), 5(5)(f).

[146] *Ibid*, s. 8.

[147] The penalty amounts are set out in column II of the schedule: See Interim Order, *supra* note 135, s. 2(1).

[148] Simon Cohen, "Canadian Recreational Drone Users Have Basically Been Grounded," *Mobile Syrup* (25 March 2017), online: < http://mobilesyrup.com > .

[149] Interim Order, *supra* note 135.

[150] See Transport Canada, "New Safety Rules for Recreational Drone Use Take Immediate Effect" (Toronto: 16 March 2017), online: < https://www.canada.ca/en/transport-canada/news > .

[151] RFID is an identification system that relies on a small chip implanted in a tag, which can record and store data: Office of Consumer Affairs, "Radio-Frequency Identification (RFID) in the Retail Marketplace" (Ottawa: OCA), online: < www.ic.gc.ca > .

legal specialist in the area, cited readability as a difficulty associated with physical plates, but agreed with the OPC that RFID could be effective.[153]

Assuming identifying information is unreadable to drone observers, it will remain unclear what can be done if a drone flies over one's home or business, as Emmett recognized pre-Interim Order. Even more crucially, it will remain unclear how operators can be identified if a drone is interfering with the path of an airliner.[154] This issue is not merely academic;[155] all regulators involved with drones to date, whether dealing with issues related to safety, security, or privacy, have recognized the need for a reliable manner by which operators can be readily identified when problems arise.[156] Unfortunately, it appears the Interim Order is both insufficiently directed towards the privacy concerns that drones present and inadequately equipped to ensure drone operators are held accountable where necessary. Although new regulations are expected to replace the Interim Order in the short term, the content of the Interim Order is presumably indicative of the form of these future regulations, suggesting deficiencies will persist.

3.2 Protecting Privacy in a Drone Age

Although safety remains the primary issue of concern for aviation regulators, drone operators must nonetheless abide by general laws regulating behaviour in society, including criminal law, privacy law, property law, and tort law. Fortunately, these laws fill some of the privacy gaps left by Transport Canada. The latter three aforementioned categories will be discussed further in the sections that follow.

3.2.1 Privacy Law

Canada has two primary privacy statutes, both of which the OPC is charged with enforcing: the *Privacy Act*,[157] which governs the personal information handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"),[158] which governs the private sector. The first difficulty with *PIPEDA* is the limited scope of the information it protects. Firstly, *PIPEDA* does not apply to recreational actors.[159] Second, the statutory cause of action under *PIPEDA* is restricted only to the loss, misuse, or unauthorized access to "personal

---

[152] OPC - Comment to Transport Canada, *supra* note 69.

[153] Peter Nowak, "Regulation of drones in Canada has yet to take off", *Canadian Business* (27 July 2016), online: < http://www.canadianbusiness.com > .

[154] *Ibid.*

[155] OPC - Comment to Transport Canada, *supra* note 69.

[156] *Ibid.*

[157] R.S.C. 1985, c. P-21.

[158] *PIPEDA*, *supra* note 67.

[159] Holden, *supra* note 12 at 105.

information"[160] that is held by an organization; thus, there is no protection conferred upon non-personal information.[161]

Where personal information is involved, collection, use, and disclosure require both the knowledge and consent[162] of the individual in question, "except where inappropriate."[163] Importantly, consent is not required where collection is for journalistic, artistic, or literary purposes.[164] *PIPEDA*'s reliance on the "utopic"[165] idea of consent has received considerable criticism, even from the OPC.[166] In a somewhat analogous activity, street-level imaging,[167] satisfaction of the consent requirement requires companies to inform citizens that they will be photographing the streets of their city.[168] Presumably, large drones can ensure compliance by doing the same.[169] Nevertheless, the OPC's position on this activity is both problematic for citizens who do not see the notice, as well as for vehicles that cannot be seen, and as a result, choose to forgo compliance. High altitude drones, which will typically be covert, are certainly problematic.[170]

---

[160] Personal information is broadly defined as "information about an identifiable individual": *PIPEDA*, *supra* note 67, s. 2(1).

[161] This contrasts with certain provincial statutory torts, which protect a broader range of privacy intrusions, and which will be discussed in Section 3.2.4.1, below. See Eric A. Dolden et al., "Current Landscape of Personal Information and Privacy Liability in Canada" (February 2016) Dolden Wallace Folick LLP, online: < http://www.dolden.com > at 8-9.

[162] Consent may be implied: *PIPEDA*, *supra* note 67, Schedule 1, s. 4.3.6; Office of the Privacy Commissioner of Canada, "Captured on Camera Street-level imaging technology, the Internet and you" (Ottawa: OPC, April 2009), online: < https://www.priv.gc.ca > at n 1 [OPC — Street-level Technology].

[163] Obtaining consent may be inappropriate, for example, where legal, medical, or security reasons create an impossibility or impracticality with regards to obtaining consent: *PIPEDA*, *supra* note 67, s. 5(1), Schedule 1, s. 4.3.

[164] *Ibid*, s. 7(1)(c); Two additional examples of available exemptions include (i) collection is in the interests of the individual and consent cannot be collected in a timely fashion; and (ii) it is reasonable to expect that collection with knowledge or consent would compromise the availability or accuracy of the information, in the event that collection was reasonable for purposes relating to investigating a breach of an agreement or the contravention of a Canadian law: *Ibid*, s. 7(1)(a)-(b).

[165] Holden, *supra* note 12 at 105.

[166] Office of the Privacy Commissioner of Canada, "Wearable Computing — Challenges and Opportunities for Privacy Protection" (Ottawa: OPC, January 2014), online: < https://www.priv.gc.ca > at para. 2(a) (technological developments pose "profound challenges" to existing privacy frameworks around the world, which are built on the idea of consent).

[167] Street-level imaging, used by Google's Street View application, involves photographing the streetscape, typically done by mounting a camera on a vehicle that is driven up and down streets: OPC — Street-level Technology, *supra* note 162.

[168] The OPC offered examples of how notice could be given, such as including visible markings on vehicles, or notifying the media: *Ibid*.

[169] Holden, *supra* note 12 at 102-104.

Indeed, even the OPC has recognized that covert surveillance,[171] an "extremely privacy-invasive form of technology,"[172] in most instances, takes place without consent.[173]

With regard to protecting against privacy intrusions by drones, *PIPEDA*'s enforcement scheme is also lacking. Firstly, as *PIPEDA* places the onus on the individual to submit a request for information or a complaint,[174] *PIPEDA* has been construed as "lax" and, therefore, not ideal for regulating privacy with respect to drones. This is particularly true, as an individual may not be aware of ensuing surveillance or of whether personal information is being captured.[175]

As Transport Canada is not considering privacy as it develops drone regulations, it is unclear precisely how *PIPEDA* will apply to drone operators.[176] Nevertheless, as the foregoing illustrates, *PIPEDA*'s ability to protect privacy as drones proliferate is certainly in question. Moreover, it is important to note that recreational users fall outside of *PIPEDA*'s scope, as *PIPEDA* limits its application to commercial actors. This was particularly troubling prior to the Interim Order, discussed in Section 3.1.1, as recreational users were excluded from regulation under both privacy legislation and civil aviation regulations; today, however, although inadequacies remain, as discussed above, the recreational use of drones does fall within the scope of the *CARs*, which represents some improvement.

3.2.2 The Common Law

Despite the statutory deficiencies mentioned above, it is important to remember that the common law governs the acts of all drone operators, as does criminal law. Although criminal law is beyond the scope of this paper, property torts, including trespass and nuisance, as well as the tort of intrusion upon seclusion, offer recourse to those that suffer privacy invasions as a consequence of drones and their surveillance capabilities. These areas of the law and the protection that they do and do not offer will briefly be considered here.

---

[170] *Ibid* at 104.

[171] There seem to be few instances in which drones would meet the OPC's requirements for performing covert surveillance at high altitudes, which suggests that such drone usage is inconsistent with *PIPEDA*. However, it is considered surprising that *PIPEDA* allows for covert surveillance in any event: See *ibid* at 102-103; See also Office of the Privacy Commissioner of Canada, "Guidance on Covert Video Surveillance in the Private Sector" (Ottawa: OPC, May 2009), online: < https://www.priv.gc.ca > [OPC — Covert Surveillance].

[172] *Ibid*.

[173] OPC — Covert Surveillance, *supra* note 171 at B.

[174] See Office of the Privacy Commissioner of Canada, "File a Complaint under PIPEDA" (Ottawa: OPC, October 2016), online: < https://www.priv.gc.ca >

[175] Bracken-Roche, *supra* note 3 at 58.

[176] Holden, *supra* note 12 at 104.

3.2.3 Property Torts: Trespass & Nuisance

Although property law provides some recourse in the event of a drone entering the airspace above private property, serious deficiencies exist in this domain as well. Beyond the complications associated with substantiating claims in trespass and nuisance,[177] standing to sue requires either ownership or exclusive possession.[178] Thus, property law offers no recourse for surveillance activities that occur in public, which are likely to be frequent in the case of drones. These torts also offer no assistance to those who are not property holders. For those that do have standing, further ambiguity awaits; although the viability of property-related claims depends on the extent and nature of the property rights held, airspace property rights have yet to be precisely defined.[179]

As aircraft have historically flown at higher altitudes, few Canadian courts have had the opportunity to consider the extent and nature of rights in airspace at lower altitudes. Taking an approach later affirmed by the leading Canadian case on the subject,[180] in *Bernstein of Leigh (Baron) v. Skyviews & General Ltd.*, the English Queen's Bench confirmed that airspace property rights are not without limit. Concluding that the defendants had not trespassed while taking a single aerial photograph of the plaintiff's country home, Justice Griffiths held that restricting airspace property rights to "such height as it is necessary for the ordinary use and enjoyment of his land and the structures upon it"[181] was most appropriate. In his opinion, such a limitation balanced individual property rights with the right of the general public to take advantage of technology.

In accordance with that reasoning, in Canada, the U.S. and the United Kingdom, airspace property rights[182] have been described as: (i) extending to the "immediate reaches" of the surface; (ii) including as much airspace as the surface owner can use or occupy; and (iii) extending as far as necessary to ensure the surface owner's full enjoyment of the land.[183] Although property rights in airspace are clearly not unlimited, where precisely airspace becomes part of the public domain is uncertain.[184] This has created "pervasive uncertainty as to

---

[177] Trespass, unauthorized interference with possession, allows both owners and lessees to make claims for intentional intrusions, even without demonstrating harm. Private nuisance, on the other hand, is unreasonable interference with one's use or enjoyment of land and does require harm, but not fault: *Ibid* at 88-89.

[178] Butler, *supra* note 11 at 444.

[179] Holden, *supra* note 12 at 84.

[180] See *Didow v. Alberta Power Ltd.*, 1988 ABCA 257, 1988 CarswellAlta 109 (Alta. C.A.) at para. 41 [*Didow*].

[181] [1978] 1 Q.B. 479, [1977] 2 All E.R. 902 (U.K. H.C.) at 488 [*Bernstein*].

[182] Note that airspace rights have been discussed in the context of power pole intrusions, using *Didow* as an example, as opposed to in the context of aircraft intrusions. Thus, the reasoning may be *obiter*: Holden, *supra* note 12 at 85.

[183] *Ibid* at 85; See generally *Lacroix v. R.*, 1953 CarswellNat 272, [1954] Ex. C.R. 69 (Can. Ex. Ct.) at 73; *Bernstein*, *supra* note 181 at 488; *Didow*, *supra* note 180 at para. 8.

[184] Holden, *supra* note 12 at 85-88.

where drones may and may not fly."[185] As property rights have only been found in airspace up to twenty metres above the land's surface in Canada,[186] property law may be incapable of capturing intrusions by even recreational drones, which can fly far higher. Accordingly, property law seems deficient in a world with drones; particularly as drones will inevitably, and imminently, fly at high altitudes and in areas where airspace property rights are non-existent, such as over public streets.

3.2.4 Actionable Privacy Rights

3.2.4.1 The Tort of Intrusion Upon Seclusion

As noted earlier, various common law causes of action have long protected privacy.[187] Despite the fact that courts were willing to protect privacy invasions by "pressing other nominate causes of action into service,"[188] Canadian courts[189] were hesitant to recognize invasion of privacy as an independently actionable wrong; thus, invasion of privacy remained "an inceptive, if not ephemeral, legal concept, primarily operating to extend the margins of existing tort doctrine."[190] Although privacy was protected indirectly, Chris DL Hunt, a widely-published academic with expertise in privacy law, argues that this resulted in a "hodgepodge" approach to privacy, which left several gaps in protection.[191]

In 2012, the ONCA recognized a need to adapt to the changing needs of society, as Warren & Brandeis had called for over a century prior.[192] With that realization, the ONCA created a new privacy tort in *Jones*: the tort of intrusion upon seclusion. Although the *Charter* only protects privacy rights vis-à-vis the State, and thus does not directly apply to private litigation,[193] the ONCA justified the creation of this new tort due to Canadian law's "explicit recognition

---

[185] Troy A. Rule, "Airspace in an Age of Drones" (2015) 90:155 BUL Rev at 170, 174.

[186] See *Didow*, supra note 180.

[187] *Jones*, *supra* note 6 at para. 15.

[188] Hunt, *supra* note 49 at 184.

[189] Note that this generalization excludes Quebec, a province which has historically been progressive in the area of privacy law. For an overview of the development of Quebec's privacy legislation, and Quebec's *Charter of Human Rights and Freedoms,* which expressly grants to each person an actionable right to privacy, see generally Paul-André Comeau & André Ouimet, "Freedom of Information and Privacy: Quebec's Innovative Role in North America" (1995) 80 Iowa L Rev 651.

[190] *Ontario (Attorney General) v. Dieleman*, 1994 CarswellOnt 151, 117 D.L.R. (4th) 449 (Ont. Gen. Div.) at 688, as cited in *Jones*, *supra* note 6 at para. 15.

[191] Hunt, *supra* note 49 at 184.

[192] See generally Warren & Brandeis, *supra* note 8.

[193] The *Charter* applies to the legislative, executive and administrative branches of government: *Charter*, *supra* note 46, s. 32; See *Dolphin Delivery Ltd. v. R.W.D.S.U., Local 580*, 1986 CarswellBC 411, 1986 CarswellBC 764, [1986] 2 S.C.R. 573 (S.C.C.) at paras. 40-41, 48 [*Dolphin Delivery*].

of a right to privacy as underlying specific *Charter* rights and freedoms, and the principle that the common law should be developed in a manner consistent with *Charter* values."[194]

Rather than adopting the reasonable expectation of privacy test as used in *Charter* jurisprudence, the statutory torts of other Canadian provinces, and in England,[195] Ontario's tort of intrusion upon seclusion is primarily based on the U.S. *Restatement* approach.[196] To protect an interest that "closely tracks" that of informational privacy,[197] as developed in *Charter* litigation,[198] *Jones* defined the key features of the cause of action as follows:

> [f]irst, that the defendant's conduct must be intentional, within which I would include reckless; second that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.[199]

Although the name of the tort, namely, its use of "seclusion," suggests that privacy interests must be "secluded" from public view to warrant protection, as required by the *Restatement*, Hunt argues that Justice Sharpe's formulation, as set out above, infers that a broad interpretation was intended,[200] which would protect privacy interests in public.[201] Nevertheless, he recognizes that the Court's references to seclusion could undermine the tort's future effectiveness.[202]

The difficulty, with the respect to the test set out above, lies in proving the third element: a "highly offensive" intrusion.[203] Such an intrusion was defined as

---

[194] John D. R. Craig, "Invasion of Privacy and *Charter* Values: The Common Law Tort Awakens" (1997), 42 McGill LJ 355, as cited in *Jones*, *supra* note 6 at para. 46.

[195] Although England does not have a discrete privacy tort for intrusions, England uses a reasonable expectation test for its modified breach of confidence tort, now described as the tort of misuse of private information: See *Mosley v. News Group Newspapers Ltd.*, [2008] EWHC 1777 (QB) (U.K. H.C.) at para. 7, as cited in *Jones*, *supra* note 6 at para. 62.

[196] Chris D.L. Hunt, "New Zealand's New Privacy Tort in Comparative Perspective" (2013) 13:OUCLJ 157 at 160 [Hunt — NZ].

[197] Recall that informational privacy refers to three distinct, although overlapping interests: privacy as secrecy, privacy as control, and privacy as anonymity: See Section 2.2.1.1.1 *supra*; See also *Spencer*, *supra* note 53 at para. 38.

[198] *Jones*, *supra* note 6 at para. 66.

[199] *Ibid* at para. 71.

[200] Chris D.L. Hunt, "Privacy in the Law: A Critical Appraisal of the Ontario Court of Appeal's Decision in *Jones v. Tsige*" (2012) 37:2 Queen's LJ 661 at 671 [Hunt — *Jones*].

[201] Hunt argues that privacy interests should be protected in public, as reasoning suggesting otherwise is "obviously specious." To him, if one loses privacy protection for venturing out in public by impliedly consenting to foreseeable intrusions, this is akin to losing property rights in baggage on an airplane, as bags commonly get lost in transit: Hunt — NZ, *supra* note 196 at 160-61.

[202] This is unlikely, however, as the SCC, the New Zealand Court of Appeal, the House of Lords, and the English Court of Appeal have rejected a strict seclusion requirement: *Ibid* at 677.

an invasion "into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive."[204] In *Jones*, this standard was met by a bank employee that viewed someone's financial records over 174 times. Importantly, this standard differs from statutory privacy torts adopted in British Columbia, Saskatchewan, Newfoundland, and Manitoba,[205] which explicitly state that privacy may be violated by surveillance.[206] Seemingly, these provinces offer a better chance for recovery.[207]

While statutory and common law torts are considered the strongest existing causes of action with respect to privacy intrusions by drones,[208] there exists an important deficiency: the combination of the cost of litigation and the nominal nature of damages likely to be awarded. In *Jones*, the ONCA awarded a mere $10,000 in damages, as Justice Sharpe made it clear that general damages were to serve a "symbolic purpose," and aggravated and punitive damages were only to be awarded in exceptional circumstances.[209] In contrast, where an ex-boyfriend posted an intimate video of the 18-year old plaintiff without her consent, $100,000 was awarded, with $25,000 being punitive in nature.[210] Nevertheless, these awards are likely to be dwarfed by the costs of litigation, taking this remedy out of reach for many.

---

[203] Hunt has criticized this "highly intrusive" requirement because privacy is inherently a dignity-based interest, which means all privacy interferences undermine a plaintiff's dignity. He further argues that the issue of "unduly sensitive litigants," which the "highly offensive" requirement is designed to preclude, is mitigated by a reasonable expectation of privacy test such as that used in the criminal/*Charter* context: *Ibid* at 164-65.

[204] *Jones*, *supra* note 6 at para. 72.

[205] See *Privacy Act*, R.S.B.C. 1996, c. 373 [B.C. *Privacy Act*]; *Privacy Act*, R.S.S. 1978, c. P-24; *Privacy Act*, R.S.N.L. 1990, c. P-22; *The Privacy Act*, C.C.S.M., c. P125 [Manitoba *Privacy Act*].

[206] See e.g., B.C. *Privacy Act*, *supra* note 205, s. 1(4); Manitoba *Privacy Act*, *supra* note 205, s. 3(a).

[207] In British Columbia, for example, successful statutory tort actions that are more analogous to potential drone surveillance include instances involving surveillance by landlords directed at a specific tenant, video recordings in bathrooms, as well as claims involving two-way mirrors and peep holes: Holden, *supra* note 12 at 95.

[208] *Ibid* at 105.

[209] *Jones*, *supra* note 6 at paras. 88-90.

[210] *Jane Doe 464533 v. D. (N.)*, 2016 ONSC 541, 2016 CarswellOnt 911 (Ont. S.C.J.) at paras. 50-53 [*Jane Doe*]. Note that *Jane Doe* was decided on summary judgment, after the defendant was noted in default. Importantly, this matter is set to be re-heard, as the defendant successfully applied for the default judgment to be set aside, and the plaintiff was unsuccessful in her appeal of that order: See *Jane Doe 464533 v. D. (N.)*, 2017 ONSC 127, 2017 CarswellOnt 163 (Ont. S.C.J.).

3.3 Conclusions on Protection

The foregoing demonstrates that the current legal framework leaves numerous gaps with respect to the protection of privacy from drone intrusions. Recreational drones, although now regulated by the *CARs*, remain outside of *PIPEDA*'s scope. Furthermore, recreational drones weighing less than 250 grams, which are not subject to the *CARs*, may be able to escape prosecution under property torts by merely flying over 20 metres in height, which they are seemingly capable of doing.[211] For SFOC-exempted commercial drones, although covert surveillance is only technically permitted in very limited circumstances, the fact that the onus is on members of the public to complain under *PIPEDA* appears to give drone operators significant leeway to operate covertly.

Moreover, while drone operators in Ontario may escape liability for surveillance completely because it is insufficiently offensive, assuming potential plaintiffs can even afford litigation, most crucially, there are numerous provinces in Canada without privacy torts at all: either statutory or common law. As courts in other provinces have been reluctant to follow in Ontario's footsteps,[212] it seems there is simply no privacy protection for intrusions in public places in those provinces. Indeed, the "hodgepodge" of common law causes of action that have historically protected privacy rights lack privacy protection as a core value, and are subject to several internal limitations.[213] For many, it seems there is simply no cause of action to be had.

4. CONCLUSION

In 1890, Warren & Brandeis recognized the need for privacy protection in response to technological advancements.[214] While *Jones* represents one manner by which the common law has evolved to address privacy concerns, at least in one Canadian province,[215] there is a clear need for the legislature to anticipate and proactively address the privacy concerns posed by drones on multiple fronts. Not only have the *CARs* been developed without regard for privacy concerns, critically, Transport Canada's regime for the identification of drones appears to

---

[211] See e.g. the Walkera Rodeo drone, which weighs less than 250 grams and has an 800-metre range, as discussed in Section 2.1.2.2, *supra*.

[212] Amanda Winters, "On Final: I spy: Drones and privacy law," *Wings Magazine* (3 March 2016), online: < https://www.wingsmagazine.com > .

[213] For example, data protection regimes do not protect those acting for a journalistic purpose, defamation, malicious falsehood, and breach of confidence requires disclosures, while trespass to the person is not available without physical touch, and property torts are only available for property holders: See Hunt, *supra* note 49 at 181-183, 184.

[214] See Warren & Brandeis, *supra* note 8.

[215] See also *Jane Doe*, *supra* note 210 at paras. 41-46 (a further tort was tentatively recognized for the public disclosure of embarrassing private facts, but the case is set to be re-heard after judgment was set aside).

be inadequate, which precludes accountability. Notably, even Transport Canada, previously a world leader in the development of regulations for the commercial use of drones, has acknowledged its inability to keep pace with the rapid development of drone technology and the growing demand for commercial drone usage.[216]

Today, technology is threatening privacy to the "point of surrender."[217] Just as computers have been recognized as a "multi-faceted instrumentality without precedent in our society,"[218] so too will be drones. Indeed, Transport Canada is pushing forward to integrate all forms of drones into society.[219] Over time, our legal system has evolved, and must continue to evolve, to address privacy concerns and the inadequacy of our laws. As this paper makes clear, with respect to drones, the shortfalls are many. Drones will undoubtedly challenge our legal system, particularly with respect to protecting privacy in public and truly defining what is anonymity and whether anonymity is even possible to protect in a world with drones.

In Kentucky, a father shot down a drone caught spying on his daughter.[220] While this precise scenario is unlikely to play out in the Canadian context, Canadian residents have already attempted to investigate the activities of drones without being able to find the appropriate government department to call.[221] As the Canadian Government has made it clear that it wishes to take advantage of the economic opportunities presented by the digital age,[222] the onus is on our legislators to ensure that members of the public, drone operators or otherwise, are protected by laws, aware of the laws, and have access to a remedy where required.

---

[216] Sheehan & Parrish, *supra* note 16.

[217] Peter Burns, "The Law and Privacy: The Canadian Experience" (1976) Can Bar Rev 1, as cited in *Jones*, *supra* note 6 at para. 67.

[218] A. D. Gold, "Applying Section 8 in the Digital World: Seizures and Searches", (Prepared for the 7th Annual Six-Minute Criminal Defence Lawyer, Law Society of Upper Canada, Toronto, 9 June 2007) at para. 3.

[219] Baxter, *supra* note 26.

[220] *Ibid.*

[221] Bracken-Roche, *supra* note 3 at 4.

[222] Government of Canada, "New Law to Protect the Personal Information of Canadians Online" (Ottawa: Industry Canada, 18 June 2015), online: < http://news.gc.ca > .