Andrew V. Shelley

Application of New Zealand Privacy Law to Drones

Introduction

There has been rapid growth in the availability and use of small-scale drones[1] in recent years, driven by the private benefits available to the drone operator. For a recreational operator the motivation may be enjoyment, but for the commercial operator there is the ability to gather information at lower cost and lower risk than previously possible, and potentially to gather information that could not previously be gathered in a cost-effective manner. Drones also give rise to a number of costs, most notably safety-related and privacy-related, which by their nature are borne by third parties. A mechanism is required for the drone operator to internalise these costs if efficient use of drones is to be achieved.

The proliferation in drone availability and use has been reflected in the number of incidents and concerns reported to the New Zealand Civil Aviation Authority. Authority statistics indicate that from 2008 to 2010 there was approximately one report per year notified to the authority. This has grown to 120 reports for the 2015 calendar year.[2] Commercial uses for drones include infrastructure inspection, surveying, general aerial photography, precision agriculture, search and rescue, and delivery services. One New Zealand study (Shelley and Andrews, 2015) estimates the potential gross benefits to be, in monetary terms: nearly $1 billion per annum from improved pasture management on sheep, beef and dairy farms; up to $95 million per annum from improved control of a common radiata pine fungus and an insect pest; and up to $7 million per annum from electricity infrastructure asset inspection, with a further benefit of up to $20 million per annum from reduced duration of power outages. Benefits not quantifiable include the ability to conduct real-time traffic monitoring (sUAS News, 2015) and activities such natural disaster response (Measure and American Red Cross, 2015).

While not common occurrences, small drones have injured people, including hitting and cutting a triathlete's head during a race (Grubb, 2014), knocking a woman unconscious at a public parade (CBS News, 2015) and injuring a baby at a public event (Henry 2015). Small drones have been used to deliver contraband to prisons in both the United Kingdom and the United States (Brandes, 2015; Glanfield, 2015); have crashed into overhead electricity lines, causing power cuts, in both New Zealand and the United States (Dinsdale, 2015; Serna, 2015); and crashed at major sporting events (Waldstein, 2015). There are concerns that small drones could be used by terrorist groups to launch bomb attacks (Hughes, 2015). Drones have been used to conduct numerous unauthorised flights

Andrew Shelley is a master's student in the School of Economics and Finance at Victoria University of Wellington, and a director of Aviation Safety Management Systems Ltd.

over French nuclear power plants, raising speculation about whether the flights are a precursor to ground-based attack (Lichfield, 2014; Baylon, 2014). Following reports that small drones have come within feet of passenger planes (see, for example, Brooks-Pollock, 2014), research has indicated that a 3.6kg drone could fracture the turbine blades of a jet aircraft, rapidly destroying the entire engine, which can potentially cause structural damage to the aircraft and even a catastrophic fire (Mackay, 2015; Wasserman, 2015; ATSB, 2013; Gates, 2015).

There has also been rising public concern about privacy issues associated with drones. New Zealand has seen newspaper articles about drones being used to film another person's property and to take photos of children at a public swimming pool (Harris, 2015; Bonnallack and Young, 2015). While the latter incident involved a father photographing his children at a school swimming sports (Bonnallack, 2015), the reporting of it highlights a general disquiet among the public about potential violation of privacy. In Australia a woman discovered that real estate advertisements, including a large billboard, carried an image of her sunbathing in her backyard (Panahi, 2014). This incident illustrates that surveillance and privacy violations can occur without trespass, such as when a drone is located over a neighbouring property or public way such as a road, footpath or walkway. It also demonstrates that privacy violations may be inadvertent: in this instance the woman happened to be sunbathing next door to the property that was the focus of the aerial footage.

There has also been rising public concern about privacy issues associated with drones.

In New Zealand the civil aviation rules currently contain a default requirement for drone operators to obtain permission to fly over persons or property (Civil Aviation Authority, 2015b, rule 101.207(a)(1)). However, civil aviation regulation is concerned solely with matters of safety, so if an operator can demonstrate a sufficient level of safety, then that restriction can be removed (Civil Aviation Authority, 2015a, p.12). Furthermore, these rules have no effect on non-trespassory surveillance. While the civil aviation rules may have incidental benefits for privacy in some situations, addressing the potential problem of privacy violations perpetrated with the aid of a drone must rely on an appropriate framework of privacy regulation.

Gavison (1980) suggests that there are three fundamental and independent elements of privacy: secrecy, anonymity and solitude. Westin (1967) argued that the control of personal information lies at the heart of privacy, but this is a facet of Gavison's secrecy. Secrecy and anonymity are arguably the foundation of New Zealand's tort of wrongful publication of private facts, and solitude the foundation of the tort of intrusion on seclusion, while the right to control personal information about oneself lies at the heart of New Zealand's Privacy Act 1993.

An additional value closely related to privacy is autonomy, which is the ability to make life decisions free from the influence or control of others (Thompson, 2015). Autonomy is a privacy value that may be threatened by widespread use of drones, as individuals feel that they must change or moderate their private behaviour in the face of potential surveillance (Martin, 2013). The perceived need to alter behaviour was demonstrated by an experiment undertaken in Helsinki, which studied the effects on ten volunteer households of ubiquitous surveillance within each home over a period of six months (Oulasvirta et al., 2012). The Helsinki Privacy Experiment demonstrated that even individuals who consent to surveillance will actively alter their behaviour in order to regulate what those carrying out the surveillance perceive, and the surveillance system was 'a cause of annoyance, concern, anxiety, and even rage'. These emotions may be sufficiently strong that individuals are motivated to undertake *prima facie* illegal behaviours, such as attempting to shoot down or otherwise destroy a drone. In the United States drones have been shot down in New Jersey, Kentucky and California. In all three cases the shooter justified their actions by claiming that they were protecting their right to privacy (Smoking Gun, 2015; Cummings, 2015; Farivar, 2015).

The negative emotions experienced by those subject to perceived privacy violations, and the behavioural responses observed in the Helsinki experiment, are economic costs to those involved. Such responses may also involve behaviours – such as the firing of a gun – that create risks, and therefore economic costs, to others. An efficient level of drone activity can only be achieved if the economic costs drones induce are taken into account by drone operators, which in turn requires a mechanism to transfer those costs to the drone operator. It is the role of the legal and regulatory system to facilitate this transfer.

The remainder of this article first summarises relevant aspects of the technology associated with drones to provide an appreciation of some of the challenges that might arise in a legal and policy context. It then considers privacy regulation in New Zealand by way of the privacy torts, the Privacy Act 1993 and other relevant legislation. The tort of intrusion on seclusion is potentially highly relevant, although there are questions over whether the threshold of 'highly offensive' will prove to be too high. The Privacy Act creates a wrong of 'interference with privacy' that is potentially applicable to drones. This article considers practical issues with enforcement and concludes with suggested clarifications to the privacy regulatory framework.

Drone technology

A drone is the colloquial name for what is officially known as a remotely piloted aircraft system or unmanned aircraft system: a flying machine without a pilot on board. In its typical use this term encompasses unmanned fixed-wing aircraft and unmanned helicopters (with

any number of rotors). A drone consists of the flying machine and the attendant control systems, which may include some means of remotely controlling the craft from a distance, such as radio control.

Whereas traditional radio-controlled aircraft are flown within sight of the operator, small drones[3] increasingly have two technologies that enable them to be flown beyond the line of sight of the operator, even though such operations are generally not legal. First, many small drones can be programmed to follow a series of GPS waypoints so that they can fly a pre-set path over points of interest. The GPS waypoints will be generated on a software application that typically uses Google Maps, so it is possible to identify with a high degree of precision a specific address, house or location that the drone is to fly to. The operator of the drone is able to watch the progress of the aircraft on a screen, without needing to physically observe the craft. Second, small drones may have 'first-person view' technology, which transmits the video from a camera mounted on the drone back to the operator. First-person view enables the operator to see the view through the drone camera and pilot the craft as if on board the drone itself.

'Nano-UAVs' (drones weighing less than 500g) may lack some of these technologies, but even a hand-sized nano-UAV weighing just 50g, including battery, is still capable of carrying a camera and operating with first-person view.[4] Some nano-UAVs have been developed specifically for surveillance purposes, mimicking birds and insects to reduce the likelihood of detection (see, for example, Ackerman, 2011).

A small drone is typically configured so that the video is broadcast back to the pilot. This imagery can be recorded. Older drones and nano-UAVs may simply record imagery on a memory card for later viewing.

New Zealand privacy law

New Zealand has two privacy torts: wrongful publication of private facts and intrusion on seclusion. These torts are heavily complemented by both civil and criminal statutes, and remain an area where further relevant development is possible. This section reviews the two privacy torts and then gives particular consideration to how the Privacy Act might apply to drones. Other relevant statute is then briefly reviewed.

Privacy torts

The confirmation of the existence of the privacy torts is a relatively new development in New Zealand law. Wrongful publication of private facts was confirmed as a tort by the Court of Appeal in *Hosking v Runting* [2004] NZCA 34. The elements of this tort are:

1. The existence of facts in respect of which there is a reasonable expectation of privacy; and
2. Publicity given to those private facts that would be considered highly offensive to an objective reasonable person.

The tort of intrusion on seclusion was found to be part of New Zealand law in the High Court in *C v Holland* [2012] NZHC 2155. Justice Whata held that the following four elements must be satisfied:

(a) An intentional and unauthorised intrusion;
(b) into seclusion (namely intimate personal activity, space or affairs);
(c) involving infringement of a reasonable expectation of privacy;
(d) that is highly offensive to a reasonable person.

What might be considered the key distinguishing factor between wrongful publication and intrusion on seclusion is that publication is not required for the latter tort. This may be particularly relevant when imagery is collected for the private use of a drone operator without necessarily an intention to publish the imagery.

Some commentators have questioned whether the tort of intrusion on seclusion is too tightly formulated. For example, Anderson (2012) notes Justice Whata's acceptance of there being 'no right to limit views from public places or from other private property', which potentially allows surveillance and photography from afar.

The 'highly offensive' test

Both privacy torts require the violation of privacy to be 'highly offensive'. In *C v Holland* the intrusion involved covert filming of a woman in the shower, so easily met the threshold of the 'highly offensive' test. In *Hosking v Runting* the action in contention was the publication of a photograph of 18-month-old twins, taken in a public place, and this did not meet the threshold. A drone filming a person sunbathing naked in their backyard might be considered an analogous situation to that in *C v Holland* and therefore likely to meet the threshold. Imagery of dead or injured persons at the scene of a traffic accident or shooting may also meet the threshold.

> New Zealand has two privacy torts: wrongful publication of private facts and intrusion on seclusion ...

Moreham (2008) argues that the 'highly offensive' test is unnecessary, noting that English law avoids the use of that test by relying on the 'reasonable expectation of privacy' test. The 'highly offensive' test is, he argues, also unpredictable and creates uncertainty. There is no easy formula to apply, with the only guidance being that the disclosure must be highly offensive to a reasonable person of ordinary sensibilities. It is unclear whether the filming of ordinary activities such as gardening or children playing games in a backyard where there is a reasonable expectation of privacy would be considered highly offensive, even if the individuals involved experienced considerable anxiety at potentially being observed.

There is considerable uncertainty over whether the privacy torts provide any effective cause of action against privacy violations by drone. The cost of bringing a claim is high, with the claimant also facing the costs of the defendant if the claim is not successful. Given the

uncertainties over success, the potentially high costs will act to deter claims and effectively allow tortious conduct to continue. In such a situation, regulation is favoured over tort (Shavell, 1984).

Privacy Act 1993

The primary regulatory instrument governing privacy in New Zealand is the Privacy Act 1993, which governs the collection, use and disclosure of personal information. The Privacy Act requires an 'agency' to comply with a set of 12 broad 'information privacy principles'. An agency is 'any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector',[5] and thus includes a drone operator, whether that operator is an individual flying recreationally or a company utilising a drone for commercial operations.

While the information privacy principles of the act do not directly create a legal right enforceable in a court of law,[6] section 66 creates a civil wrong of 'interference with privacy'. Interference with privacy requires that the action in question breaches an information privacy principle (or one of four other specified breaches)[7] and in the opinion of the privacy commissioner or the Human Rights Review Tribunal has caused or may cause some harm to the individual. An action in the tribunal may be at the suit of either the director of human rights proceedings (Privacy Act 1993, section 82) or the aggrieved party (section 83), and may be appealed to the High Court.[8] The aggrieved party may only bring suit after the Office of the Privacy Commissioner has investigated the complaint, and the scope of the tribunal's hearing is restricted to the issues investigated by the privacy commissioner.

In both New Zealand and the United Kingdom unmanned aerial systems are considered to be a form of closed circuit television (CCTV) and subject to the same privacy regulation as CCTV (Mabbett, 2015; Information Commissioner's Office, 2015). In *Armfield v Naughton* [2014] NZHRRT 48, the tribunal considered issues related to a CCTV system that in part surveilled the front yard of a neighbouring property. Naughton had set up a number of CCTV security cameras around his house, one of which had an unobstructed view of Armfield's lawn and of the swing used by Armfield's children. The tribunal held that the camera recording part of the front yard collected personal information in a way that intruded to an unreasonable extent on the personal affairs of the people living at Armfield's property. Whether the surveillance was 'highly offensive' as required by the privacy torts was not considered by the tribunal as its jurisdiction is limited to the Privacy Act.

> … real estate photography is a lawful purpose, but it is unclear whether the use of a drone to collect that imagery intrudes to an unreasonable extent on the privacy of a person in a neighbouring property.

Armfield v Naughton confirmed previous decisions that 'injury to feelings' includes negative feelings such as anxiety, stress, fear and anger; that is, all of the feelings associated with unwelcome surveillance. Damages were awarded for 'humiliation, loss of dignity, and injury to the feelings of the aggrieved individual'. A benchmark of $15,000 in damages was noted by the tribunal, although a lesser amount was awarded effectively at the request of the plaintiff.

Personal information is defined in the Privacy Act as 'information about an identifiable individual'. Whether an individual can be clearly identified from drone imagery depends on the quality of the camera on board the drone and the distance between the drone and the person. A person on the ground is unable to determine whether photography is occurring, or whether they can be identified from any imagery. Furthermore, when the address at which imagery is taken is known, it may be possible to identify the individual from certain characteristics such as build and hair colour. Thus, even when the imagery is at a relatively low resolution, it is reasonable to assume that personal information is being gathered.

We can therefore conclude that (1) a drone that flies in the vicinity of a property and takes photos of that property is potentially collecting personal information; and (2) a person who is in some way upset, anxious or angry about such an action has suffered an 'injury to feelings'. Having satisfied the second limb of section 66, the only remaining requirement to prove an interference to privacy is whether the personal information collected breaches an information privacy principle.

Information privacy principle 1 requires that 'the information is collected for a lawful purpose connected with a function or activity of the agency, and the collection of information is necessary for that purpose'. Flying a drone recreationally is not an unlawful purpose, but it is not clear that collection of personal information by way of imagery is necessary for that purpose. Further, personal information may be collected incidentally when a drone is collecting imagery of an entirely different subject, and it is unclear whether this would contravene this principle.

Information privacy principle 4 requires, *inter alia*, that personal information shall not be collected by an agency 'by means that, in the circumstances of the case … intrude to an unreasonable extent upon the personal affairs of the individual concerned'. Whereas intrusion on seclusion requires the intrusion to be 'highly offensive', the Privacy Act merely requires the collection of information to intrude to 'an unreasonable extent'. The Office of the Privacy Commissioner notes that it is almost certainly unreasonably intrusive to capture imagery of 'a person's private front or back yard or any other place where they are likely to expect privacy' (Privacy Commissioner, 2009, p.13), a position upheld in *Armfield v Naughton*.

The Australian sunbathing incident (Panahi, 2014) is illustrative of some of the difficulties faced in applying the Privacy Act to drones: real estate photography is a lawful purpose, but it is unclear whether the use of a drone to collect that imagery intrudes to an unreasonable extent on the privacy of a person in a neighbouring property. However, there may be an arguable case for an unreasonable intrusion when imagery is deliberately collected about an individual or property but consent has not been obtained, such as occurred in *Armfield v Naughton*.

Information privacy principle 6 requires that where an agency holds personal information in a form that can be readily retrieved, the individual concerned has a right to obtain confirmation of whether information is held and to access that information (i.e. view the footage that pertains to the individual). However, enforcing that right may be difficult, as it may be difficult to identify the drone operator.

In sum, footage deliberately collected without permission of someone's front or backyard is likely to breach at least one information privacy principle and thus might be an 'interference with privacy', but the status of information collected incidentally to a lawful purpose is unclear.

Crimes Act and Summary Offences Act

Part 9A of the Crimes Act 1961 creates a number of 'crimes against personal privacy', including interception of private communications, disclosure of private communications unlawfully intercepted, and making, possessing and distributing intimate visual recordings. An intimate visual recording is one made without the knowledge or consent of the person who is the subject of the recording, where the recording is of a person who is in a place that would reasonably be expected to provide privacy, and the person is engaged in an activity of an intimate or personal nature, or the recording is made from under a person's clothing. Such conduct must be intentional or reckless. Of note, an intimate visual recording can be made and transmitted in real time without retention or storage.

The prohibition against intimate visual recordings has potential application in some of the more extreme situations that might be envisaged involving drones. In the Australian sunbathing case, for example, the woman was in a place (a fenced backyard) that would reasonably be expected to provide privacy, and her state of dress meets the test in section 216G of the act. An important question is whether the conduct was intentional or reckless.

Section 30 of the Summary Offences Act 1981 creates an offence punishable by a fine of not more than $500 for 'peeping or peering into a dwelling house' at night. The offences of interception of private communications and peeping or peering into a dwelling house are additional to the actions available in tort,[9] but in general would be of little help to those concerned about an unwanted drone hovering over their house or property because in most instances a drone will be gathering imagery rather than intercepting communications, and significant surveillance can be conducted without peeping into a house at night.

> The general public is concerned about the ability of drones to violate their privacy and surveil activities conducted in spaces where people have a reasonable expectation of privacy.

Discussion

People are generally concerned about their right to privacy, and unwelcome surveillance both impinges on this right and generates a range of emotions and changes in behaviour that can rightly be characterised as economic costs. The appropriate place to address issues of privacy and unwelcome surveillance lies within privacy law.

New Zealand's privacy torts require the publication or recording of information to be 'highly offensive', a threshold that is unclear for observation of people undertaking normal activities in their backyards. The Privacy Act provides an alternative cause of action for an 'interference with privacy'. Imagery collected over time by CCTV of private front and backyards has been held to intrude to an unreasonable extent on privacy, and thus constitute an interference with privacy, but it is unclear whether a single drone flight collecting the same imagery would necessarily constitute an unreasonable intrusion.

It is generally accepted that one 'can take and/or publish photos or film of people where there is no expectation of privacy, such as a beach, shopping mall, park or other public place' (New Zealand Police, 2016). However, Moreham suggests that the expectation of privacy in public places is a matter of degree, such that an individual will choose how much of themselves to reveal in any given public place, and 'because it is always possible to disseminate an image of a person to a much wider audience than the one to which he or she was exposed' (Moreham, 2006). There may, therefore, be circumstances in which drone imagery obtained in a public place may violate a reasonable expectation of privacy.

A significant difficulty also arises in identifying the pilot of a drone (Aldworth, 2014). Manned aircraft are required to have prominently displayed registration marks, or an approved and readily identifiable paint scheme, and are large enough that visible markings can be easily identified. A drone, on the other hand, may be a generic off-the-shelf model that looks exactly the same as every other drone of that model, with no unique identifying marks that are readily visible. While regulation could require that a drone has some sort of registration marking, such regulations could be ignored almost with impunity. Furthermore, even if a drone

has a registration marking, the small size of the craft means that the registration marking will necessarily be small, inhibiting identification. The pilot may also not be visible to the occupier of the property, particularly if flying using first-person view.

Two additional problems arise that reduce the expected damages cost to the drone operator. The first problem is one of asymmetric information: the potential victim does not know whether they are being recorded, which raises uncertainty over whether it is worth the cost of initiating an action or making a complaint to the privacy commissioner, particularly as the privacy commissioner has held that if a drone is not recording then there is no information collected, so no information privacy principle can be violated (Privacy Commissioner, 2015). The second problem is that there is no guaranteed cause of action. An intrusion into seclusion must be highly offensive for an action in tort, and yet the boundary of that standard is undefined; an intrusion into seclusion must also be intentional, and the drone operator always has the opportunity to argue that any intrusion was unintentional or negligent. Similarly, an 'interference with privacy' requires the drone to have intruded to an unreasonable extent in the collection of personal information, and again relies on asymmetric information about whether information was even collected.

Faced with such uncertainties, a smaller proportion of cases will be pursued than would be the case if there were certainty about the filming, and some of the cases that are pursued will fail. As discussed earlier, the probability of identifying the pilot is also very low. As a consequence of these factors, the expected damages cost borne by the drone operator will be a small fraction of the harm caused, and the drone operator will accordingly exercise insufficient care to avoid privacy violations. This can only be an efficient outcome if the cost of reducing or eliminating the uncertainty is very high and there are no other options for protecting privacy, such as destruction of the offending drone (for a discussion of the potential use of 'violent self-defence' against drones see Froomkin and Colangelo, 2015).

In sum, there are sufficient uncertainties in the application of the current body of tort and statute that a person upset by unwelcome surveillance cannot be sure of an acceptable resolution, even when that surveillance takes place in a location where they have a reasonable expectation of privacy. From an economic perspective this imposes uncompensated costs on the victim. More importantly, because the drone operator does not face the cost of his or her actions, he or she will not take sufficient precaution to avoid privacy violations and will have an activity level that is too high (Shavell, 1980).

Conclusion

The general public is concerned about the ability of drones to violate personal privacy and surveil activities conducted in spaces where people have a reasonable expectation of privacy. Experimental evidence demonstrates that even individuals who consent to surveillance experience a range of negative emotions, including fear, anxiety and anger, and change their behaviours in response to surveillance. These negative emotions and the behaviour changes are economic costs that must be taken into account when determining the efficient use of drones.

An efficient outcome could in theory be achieved via tort. However, New Zealand's privacy torts may set too high a standard ('highly offensive'), and in any event this standard would need to be tested in court to definitively determine what level of drone surveillance meets the threshold. The costs of such action are high, effectively preventing tort from acting as an efficient mechanism for addressing privacy violations. The Privacy Act's offence of an 'interference with privacy' potentially provides a mechanism that more readily facilitates the transfer of cost to the drone operator. However, the privacy commissioner has held that if a drone is not recording imagery then no 'collection' occurs, and hence no interference with privacy occurs. This provides the obvious incentive for any drone operator subject to a Privacy Act complaint, but who has not actually published imagery, to simply claim that no information was collected. Additional problems may arise in identification of the drone operator.

This article has identified areas where New Zealand's current privacy framework requires clarification to better accommodate the challenges posed by drones. Some of the modifications could potentially be achieved by way of a code of practice issued under the Privacy Act, which may provide a relatively low-cost means of setting the standard of acceptable behaviour. Challenges will still remain because the characteristics of drone technology make it difficult to identify the operator, which in turn makes it difficult to obtain any legal remedy. Such challenges may mean that in some instances an alternative, more direct means of intervening to protect one's right to privacy would be efficient.

1 The term 'drone' is a colloquial expression for an unmanned aircraft that may be variously known as an unmanned aerial vehicle (UAV) or a remotely piloted aircraft (RPA). The term drone may also be used for the complete 'system' that encompasses the flying machine, telemetry links and ground control station, otherwise known as an unmanned aerial system (UAS) or remotely piloted aircraft system (RPAS).
2 These reports may cover any aspect of drone activities, including crashes, close approaches to manned aircraft, operating in airspace where there is no authorisation.
3 In the context of UAVs, 'small' is typically taken to mean 25kg or less (US Department of Transportation, 2013).
4 The author owns a JJRC H6C quadcopter which has an all-up weight of 50g, including quadcopter, battery and propeller guards. The H6C is fitted with a 2MP camera that records still photos or video to a micro-SD card. A different model of this quadcopter is fitted with FPV capabilities.
5 The definition of agency in the Privacy Act also includes a number of exceptions, none of which rule out a private individual collecting information about others.
6 Section 11 of the Privacy Act expressly provides that 'the information privacy principles do not confer on any person any legal right that is enforceable in a court of law', with the exception to obtain confirmation from a public sector agency of whether information is held, and to have access to that information.
7 The other breaches specified in section 66 of the act are a breach of: (a) a code of practice relating to public registers; (b) an IPP or code of practice related to information sharing agreements; (c) an information sharing agreement; and (d) provisions relating to information matching.
8 Appeals to the High Court are made under section 123 of the Human Rights Act 1993.
9 Section 405 of the Crimes Act 1961 expressly provides that 'no civil remedy for an act or omission shall be suspended by reason that such act or omission is an offence'.

Acknowledgements

This article is derived from material to form a master's degree in the School of Economics and Finance, Victoria University of Wellington, supervised by Professor Lewis Evans. I would like to thank Dr James Every-Palmer and an anonymous reviewer for helpful comments and suggestions. All errors are those of the author. Address for correspondence: Andrew.Shelley@xtra.co.nz.

References

Ackerman, E. (2011) 'AeroVironment's Nano Hummingbird surveillance bot would probably fool you', *IEEE Spectrum*, 4 March

Aldworth, N. (2014) Testimony of Chief Inspector Nick Aldworth of the Metropolitan Police before the House of Lords select committee on the European Union inquiry on civil use of remotely piloted aircraft systems (RPAS), 17 November

Anderson, N.C. (2012) 'A new frontier for privacy law?', ChenPalmer.com, 19 September, retrieved from http://www.chenpalmer.com/news/news-articles/a-new-frontier-for-privacy-law/

Armfield v Naughton [2014] NZHRRT 48

ATSB (2013) *In-flight Uncontained Engine Failure Airbus A380-842, VH-OQA*, aviation occurrence report AO-2010-089, ATSB Transport Safety Report, Australian Transportation Safety Bureau, 27 June

Baylon, C. (2014) 'Drones: the threat to nuclear plants', *Newsweek*, 27 December

Bonnallack, A. (2015) 'Dad used drone to snap his children', *Wairarapa Times-Age*, 3 March

Bonnallack, A. and A. Young (2015) 'Mystery drone hovers over pool', *Wairarapa Times-Age*, 2 March

Brandes, H. (2015) 'Drone carrying drugs, hacksaw blades crashes at Oklahoma prison', *Reuters*, 27 October

Brooks-Pollock, T. (2014) 'Drones "could be used as flying bombs for terror attack on passenger jet"', *Telegraph*, 12 December

C v Holland [2012] NZHC 2155; [2012] 3 NZLR 672 (24 August 2012)

Civil Aviation Authority (2015a) Advisory Circular AC102-1: unmanned aircraft – operator certification, revision 0, 27 July

Civil Aviation Authority (2015b) *Civil Aviation Rules Part 101: gyrogliders and parasails, unmanned aircraft (including balloons), kites, and rockets – operating rules*, 24 September

CBS News (2015) 'Falling drone knocks woman out at Seattle pride parade', *CBS News*, 30 June

Cummings, R. (2015) 'Hillview man arrested for shooting down drone; cites right to privacy', *WDRB News*, 1 August

Dinsdale, M. (2015) 'Operator investigated after drone hits lines', *Northern Advocate*, 23 September

Farivar, C. (2015) 'Man shoots down neighbor's hexacopter in rural drone shotgun battle', *ARS Technica*, 28 June, retrieved from http://arstechnica.com/tech-policy/2015/06/man-shoots-downs-neighbors-hexacopter-in-rural-drone-shotgun-battle/

Froomkin, A.M. and Z. Colangelo (2015) 'Self-defence against robots and drones', *Connecticut Law Review*, 48 (1)

Gates, D. (2015) 'Engine parts pierced protective case in British Airways 777 fire in Las Vegas', *Seattle Times*, 11 September

Gavison, R. (1980) 'Privacy and the limits of the law', *Yale Law Journal*, 89 (3), pp.421-71

Glanfield, E. (2015) 'Drone that makes getting drugs and illicit mobile phones in Strangeways "as easy as ordering Chinese" crashes inside prison yard', *Mail Online*, 9 November

Grubb, B. (2014) '"River of blood" after drone "hits" Australian athlete', *Sydney Morning Herald*, 7 April

Harris, C. (2015) 'Drones invading our privacy say critics', www.stuff.co.nz, 25 January

Henry, J. (2015) 'Falling drone injures 11-month old near Pasadena City Hall', *Pasadena Star-News*, 15 September

Hosking v Runting [2004] NZCA 34 (25 March 2004)

Hughes, C. (2015) 'ISIS planning to use toy helicopters as bombing drones fear security chiefs', *Mirror*, 22 July

Information Commissioner's Office (2015) *In the Picture: a data protection code of practice for surveillance cameras and personal information*, version 1.1, 21 May

Lichfield, J. (2014) 'French government on high alert after unexplained drone flights over nuclear power stations', *Independent*, 10 November

Mabbett, C. (2015) 'Game of drones', privacy commissioner blog, 21 January, retrieved from https://www.privacy.org.nz/blog/drones/

Mackay, S. (2015) 'Engineering researchers seek remedies for threat posed by drones to commercial airliners', *Virginia Tech News*, 28 October, retrieved from http://www.vtnews.vt.edu/articles/2015/10/102815-engineering-jetenginedronestrike.html

Martin, A. (2013) 'Privacy and surveillance primer', *Novatica*, special English edition: Privacy and the New Technologies, 2012/13 annual selection of articles, 11–15, p.1, retrieved from http://www.ati.es/novatica/2013/ASA/NvS2013-Digital.pdf#page=13

Measure and American Red Cross (2015) *Drones for Disaster Response and Relief Operations*, April

Moreham, N.A. (2006) 'Privacy in public places', *Cambridge Law Journal*, 65, pp.606-35

Moreham, N.A. (2008) 'Why is privacy important? Privacy, dignity and development of the New Zealand breach of privacy tort', in J. Finn and S. Todd (eds), *Law, Liberty, Legislation,* LexisNexis NZ

New Zealand Police (2016) 'What are the rules around taking photos or filming in a public place?', retrieved from http://www.police.govt.nz/faq/what-are-the-rules-around-taking-photos-or-filming-in-a-public-place

Oulasvirta, A., A. Pihlajamaa, J. Perkiö, D. Ray, T. Vähäkangas, T. Hasu, N. Vainio and P. Myllymäki (2012) 'Long-term effects of ubiquitous surveillance in the home', *Proceedings of the 14th International Conference on Ubiquitous Computing,* pp.41-50

Panahi, R. (2014) 'Mt Martha woman snapped sunbaking in g-string by real estate drone', Herald Sun, 17 November

Privacy Commissioner (2009) *Privacy and CCTV: a guide to the Privacy Act for businesses, agencies and organisations,* Wellington: Office of the Privacy Commissioner

Privacy Commissioner (2015) 'Case Note 267458 [2015] NZ PrivCmr 6: man objects to drone filming near his apartment', 12 August

Serna, J. (2015) 'Drone knocks out power to hundreds of West Hollywood residents', *Los Angeles Times,* 27 October

Shavell, S. (1980) 'Strict liability versus negligence', Journal of Legal Studies, 9 (1), pp.1-25

Shavell, S. (1984) 'Liability of harm versus regulation of safety', *Journal of Legal Studies,* 13 (2), pp.357-74

Shelley, A. and H. Andrews (2015) *Economic Benefits to New Zealand from Beyond-Line-of-Sight Operation of UAVs,* final report, 10 February, prepared for Callaghan Innovation

Smoking Gun (2015) 'Man indicted for shotgun blasts at hovering drone', 25 August, retrieved from http://www.thesmokinggun.com/documents/crime/new-jersey-drone-shooting-case-213450

sUAS News (2015) 'Dutch government successfully uses Aerialtronics drones to control traffic', sUAS News.com, 1 July, retrieved from http://www.suasnews.com/2015/07/36906/dutch-government-successfully-uses-aerialtronics-drones-to-control-traffic/

Thompson, R.M. (2015) *Domestic Drones and Privacy: a primer,* Congressional Research Service, R43965, 30 March

US Department of Transportation (2013) *Unmanned Aircraft Systems (UAS) Service Demand 2015-2035: literature review and projections of future usage,* technical report DOT-VNTSC-DoD-13-01, prepared for United States Air Force, version 0.1, John A. Volpe National Transportation Systems Center, US Department of Transportation, September

Waldstein, D. (2015) 'Drone crash interrupts match', *New York Times*, 3 September

Wasserman, S. (2015) 'Personal drones getting sucked into jet engines could be disastrous', Engineering.com, 3 November, retrieved from http://www.engineering.com/DesignSoftware/DesignSoftwareArticles/ArticleID/10914/Personal-Drones-Getting-Sucked-into-Jet-Engines-Could-Be-Disastrous.aspx

Westin, A. (1967) *Privacy and Freedom*, New York: Atheneum