

ASHLEY M VARNEY

THE TAKE-OFF OF DRONES

**Developing the New Zealand torts of privacy to meet the
rise in civilian drone technology**

Submitted for the LLB (Honours) Degree

Faculty of Law

Victoria University of Wellington

2016

Abstract

This paper assesses the privacy ramifications associated with the rise in the use of civilian drone technology. It discusses the capabilities of drones to take photographs, record videos and undertake ongoing surveillance, and distinguishes these capabilities from previous similar technologies such as CCTV and standard cameras. It is argued that the current approach to the New Zealand privacy torts is not adequate to allow for effective claims when breaches of privacy occur by drone operators. It is advocated that the theoretical premise of the torts, and the overall protection of privacy, is best served by emphasis on both a normative and multifaceted approach to the test of a reasonable expectation of privacy where drones are concerned. Moreover, privacy breaches by drones may be undermined by the highly offensive requirement found within both torts, as well as the mental element of intention found within the C v Holland tort.

Keywords: "Drones", "Privacy", "Tort", "Wrongful Publication of Private Facts", "Intrusion into Seclusion".

Contents

I	INTRODUCTION	4
II	UNDERSTANDING PRIVACY	5
	A What is ‘Privacy’?	5
	B Why is Privacy Important?	6
III	PRIVACY IMPLICATIONS OF DRONES	9
	A What Are Drones?	9
	B A New Privacy Threat	11
IV	DEVELOPING THE PRIVACY TORTS	14
	A Current Scope of the Torts.....	14
	B Reasonable Expectation of Privacy	16
	1 Normative approach.....	17
	2 Multifaceted approach	18
	(a) Location.....	19
	(b) Method of intrusion or acquisition of the information.....	21
	(c) Depiction of the information.....	23
	(d) Nature of the activity or information.....	25
	C Highly Offensive	27
	D Mental Element.....	28
V	CONCLUSION	30
VI	BIBLIOGRAPHY	33

I Introduction

The world's exponential increase in technologies used to watch, record and dissect our every move is challenging traditional notions of privacy. The growth in the availability and use of drone technology has afforded operators the ability to accumulate personal information at low cost and low risk, in a way that threatens to perfect the art of photography and recording.¹ Whilst the various applications of civilian drones provide military, commercial and recreational benefits, the novelty of drones has precipitated a regulatory crisis; causing law-makers to scramble to meet the legal threats that drones pose. Broadly, there is the discernible question of how the law ought to respond to drones. This paper provides an analysis of one type of legal response that pertains directly to the privacy implications of drones: the New Zealand torts of privacy.

The impetus for this paper derives from the ordinary person with the natural human desire to maintain privacy and exercise a choice in respect of the incidence and degree of their social isolation.² The inquiry at the heart of this paper is how the New Zealand courts ought to develop the torts of 'wrongful publication of private facts' and 'intrusion into seclusion' where drones challenge the human aspiration of privacy. It will do this first by examining how the development of the torts is necessitated on a theoretical basis, which will warrant an analysis of the capabilities of drones and the resulting privacy implications. As discussed in Part III, drones have various functions but this paper is primarily concerned with civilian drones equipped with photographing and video-recording capabilities. Secondly, this paper will consider how the privacy torts ought to be adapted and applied to the modern context of drones in order to achieve their underlying purposes. Such development will include reference to a normative and multifaceted approach to the test of a 'reasonable expectation of privacy', a reformulation of the 'highly offensive' test contained within both torts, and a reappraisal of the mental requirement of the torts.

¹ M. Ryan Calo "The Drone as Privacy Catalyst" (2011) 64 Stan L Rev 29 at 30.

² *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [264].

II *Understanding Privacy*

A *What is 'Privacy'?*

Originally articulated by Brandeis J as “the right to be let alone”, privacy provides for the protection of people’s “thoughts, sentiments and emotions”.³ Essentially, privacy refers to “a state of personal exclusion from involvement with or the attention of others”,⁴ or as Moreham describes it, a state of “desired inaccess”.⁵ ‘Access’ refers to seeing, hearing, touching, coming within physical proximity or obtaining information about someone.⁶ Inaccess must be ‘desired’ because people may be inaccessible but not in a state of privacy as society understands it.⁷ Withdrawal from society may be realised through physical or psychological means or through a condition of anonymity or reserve.⁸

However privacy is not a stagnant concept, nor does it operate in the abstract. Westin asserts that discussion about how best to protect privacy shifts in an age where so many forces of science, technology and society press against it.⁹ In the technological age, privacy has become so informationally enriched that current notions of privacy often revolve around the claim of people to determine “when, how, and to what extent information about them is communicated to others”.¹⁰ The New Zealand privacy torts relate to both informational and physical privacy (unwanted sensory access).¹¹ Privacy is thus a sweeping concept, including freedom of thought, control over one’s body, freedom from surveillance, protection from dissemination of personal information, and protection from searches and interrogations, peeping, eavesdropping or wiretapping.¹²

³ Samuel D. Warren and Lewis D. Brandeis “The Right to Privacy” (1890) 4 Harv L Rev 193 at 205.

⁴ *Hosking v Runting*, above n 2, at [264].

⁵ N.A. Moreham “The Protection of Privacy in English Common Law: a doctrinal and theoretical analysis” (2005) 121 LQR 628 at 636.

⁶ N.A. Moreham “Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort” in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation* (LexisNexis, Wellington, 2008) 231 at 232.

⁷ At 232. See also Charles Fried “Privacy” (1968) 77 Yale LJ 475 at 482.

⁸ Alan F. Westin *Privacy and Freedom* (Atheneum, New York, 1967) at 7.

⁹ At 3.

¹⁰ At 7.

¹¹ N.A. Moreham “Beyond Information: Physical Privacy in English Law” (2014) 73 CLJ 350 at 353.

¹² Daniel J. Solove *Understanding Privacy* (Harvard University Press, Cambridge, 2008) at 1.

B Why is Privacy Important?

This paper will defend privacy as a right that is worthy of protection, despite contention that privacy is not always socially beneficial, in that it is a plea for the right to misrepresent oneself to the rest of the world.¹³ Not all violations of privacy will be actionable. There may be instances where privacy breaches are not of the kind that warrant protection, or are justified on the basis that publication of the information is of legitimate public concern in a free and democratic society. Understanding the circumstances where tortious liability might arise in the context of drones requires consideration of the underlying tenets of the privacy torts. Privacy breaches cause harm, and as Moreham points out, “both physical and informational privacy breaches undermine the claimant’s dignity, autonomy and relationships”, leading to feelings of “distress, mistrust and violation”.¹⁴

Privacy breaches engender harm of the type described by Warren and Brandeis as incorporeal rather than physical injury.¹⁵ Modern technology has, through invading a person’s privacy, “subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury”.¹⁶ One form of harm, objective privacy harm, is actual adverse consequences that materialise external to the person. People want to protect personal activities, such as going to the bathroom or undressing, or information that makes them vulnerable or that can be used against them to produce physical, emotional, financial, or reputational harm.¹⁷ Reputation and character are important because they are indispensable to self-identity and the currency through which people interact with others and engage in public life.¹⁸ Disclosure of private information can be particularly deleterious because it makes a person a prisoner of his or her recorded past,¹⁹ potentially affecting long-term wealth, prosperity, security and employment.²⁰ The harm is worse

¹³ At 5.

¹⁴ Moreham, above n 11, at 370.

¹⁵ Warren and Brandeis, above n 3, at 196.

¹⁶ At 196.

¹⁷ M. Ryan Calo “The Boundaries of Privacy Harm” (2011) 86 Ind LJ 1131 at 1143.

¹⁸ Daniel J. Solove “A Taxonomy of Privacy” (2006) 154 U Pa L Rev 477 at 551.

¹⁹ At 533.

²⁰ At 551.

when privacy breaches provide inaccurate assessments of an individual leading to misimpressions and condemnation without full understanding.²¹ Here the individual is not even accountable for the information released and thus has less influence over the privacy breach.

Mental, or subjective, harm arises where there is a perception of loss of control that results in fear or discomfort,²² or what may be termed “injury to the feelings”.²³ Subjective harm need not occur in the moment; in fact many feelings of violation have a delayed effect,²⁴ for example where a victim does not realise a drone is recording but is caused discomfort or anguish upon discovery weeks later.²⁵ Greater harm occurs where observation is systematic due to the intensified ‘creepiness’ or violation and the chilling effects on people’s behaviour. Emotional harm may not arise exclusively from actual observation, but also from the mere belief that one is being observed.²⁶ This makes people less likely to engage in activities that they are socialised to conceal, or that might cause embarrassment or humiliation.²⁷ As explored by Foucault, prisoners behave and comply with rules not just because they are actually being observed, but because they believe they might be.²⁸ If an individual is aware of a drone operating within proximity of their space, harm may therefore arise whether or not that drone is taking photos or recording footage when it flies.

Aside from harm, individuals value privacy because it promotes a number of other ends essential for human flourishing.²⁹ Privacy is a bulwark for the autonomous self.³⁰

²¹ At 533.

²² Calo, above n 17, at 1143.

²³ Warren and Brandeis, above n 3, at 197.

²⁴ Calo, above n 17, at 1145.

²⁵ This would be akin to *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672 where the plaintiff was unaware she was being recorded at the time of the violation, but harm was caused upon later revelation of the footage.

²⁶ Calo, above n 17, at 1146. See also M. Ryan Calo “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship” (2010) 114 Penn St L Rev 809 at 842-48.

²⁷ Solove, above n 18, at 536.

²⁸ Michel Foucault *Discipline and Punish: The Birth of the Prison* (2nd ed, Vintage Books, New York, 1975) at 200-01.

²⁹ Moreham, above n 6, at 233.

Autonomy is the power to exercise independent moral judgment or make rational decisions, even when such judgment is unpopular.³¹ As Thomas J stated in *Brooker v Police*, “it is within a person’s sphere of privacy that the person nurture his or her autonomy and shapes his or her individual identity”.³² The retreat into private spaces or the ability to withhold certain information facilitates emotional release and promotes liberty of thought and action.³³ Autonomy creates space for the work of self-making,³⁴ through which one can engage in learning, creation and questioning.³⁵ Privacy is thus not a negative value, i.e. solely a ‘freedom from’, but a positive interest, the ‘freedom to’ act in a particular way.³⁶ Such freedom is a precondition for meaningful informed citizenship,³⁷ and thus to a functioning democratic society.

Moreover, aspects of people’s lives should remain private so as to protect them from violations of human dignity.³⁸ Dignity refers to the ability to command attitudinal respect.³⁹ In their seminal article, Warren and Brandeis articulated the communitarian goal of privacy, being to protect “the forms of respect that we owe to each other as members of a common community”.⁴⁰ As S. Benn notes, individuals should not be treated as “objects or specimens” to be found out about, but rather subjects with sensibilities, ends and aspirations of their own.⁴¹ Case law has also long recognised the relationship between privacy and dignity. Tipping J in *Hosking v Runting* rightly stated that “[i]t is of the essence of the dignity and personal autonomy of all human beings that some aspect of their lives should be able to remain private if they so wish”.⁴² In *Campbell v Mirror*

³⁰ Julie E. Cohen “What Privacy is For” (2013) 126 Harv L Rev 1 at 4.

³¹ Ruth Gavison “Privacy and the Limits of Law” (1980) 89 Yale LJ 421 at 449.

³² *Brooker v Police* [2007] NZSC 30, [2007] 3 NZLR 91 at [182].

³³ Moreham, above n 6, at 233.

³⁴ Cohen, above n 30, at 7.

³⁵ Gavison, above n 31, at 448.

³⁶ Wendell B. Alcorn Jr “Reviews” (1968) 6 Hous L Rev 200 at 201.

³⁷ Cohen, above n 30, at 2.

³⁸ *Hosking v Runting*, above n 2, at [239].

³⁹ Robert C. Post “Three Concepts of Privacy” (2001) 89 Geo LJ 2087 at 2092.

⁴⁰ Robert C. Post “Rereading Warren & Brandeis: Privacy, Property and Appropriation” (1991) 41 Case W Res L Rev 647 at 650-651.

⁴¹ S. Benn “Privacy, Freedom, and Respect for Persons” in J. Roland Pennock and John W. Chapman (eds) *Privacy: NOMOS XIII* (Atherton Press, New York, 1971) 1 at 6-7.

⁴² *Hosking v Runting*, above n 2, at [239].

Group Newspapers Ltd Lord Hoffman said that modern English privacy law concerns “the right to control the dissemination of information about one’s private life and the right to the esteem and respect of other people”.⁴³ Privacy intrusions disregard a person’s choice as to when and by whom he or she is accessed and also disregard the subject’s wellbeing and peace of mind.⁴⁴

III Privacy Implications of Drones

A What Are Drones?

Originally the preserve of military for reconnaissance and combat purposes, the idea of ‘drones’ (otherwise known as ‘Unmanned Aerial Vehicles’ or ‘Remotely Piloted Aircraft Systems’) is not completely new. Drones are flying machines that are accompanied by an attendant control system that allows the aircraft to be controlled from the ground, aided by computer algorithms.⁴⁵ They are essentially robots, with little decision-making ability of their own.⁴⁶

Different categories of civilian drones, from larger fixed-wing aircrafts to tiny quadcopters, can be distinguished according to factors such as size, form, shape, speed and mass.⁴⁷ Civilian applications of drones are extensive, ranging from crime fighting, environmental monitoring of whalers, aerial delivery services, checking electricity cables and pipelines, search and rescue, and real estate aerial photography, to private recreational uses such as amateur photography and video making.⁴⁸ Some drones have the primary function of pickup and delivery, such as the proposed conceptual drone-based delivery system called ‘Amazon Prime Air’, whilst others have a primary function that involves

⁴³ *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22, [2004] 2 AC 457 at [51].

⁴⁴ Moreham, above n 6, at 236.

⁴⁵ Andrew V. Shelly “Application of New Zealand Privacy Law to Drones” (2016) 12 Policy Quarterly 73 at 75.

⁴⁶ Sarah A. Hinchliffe “Drones - a ‘Serious’ Invasion of Privacy in the Digital Era?” (2014) 11 PrivLB 155 at 156.

⁴⁷ At 156.

⁴⁸ At 155.

recording or photographing.⁴⁹ It is the latter type of drone that poses the greatest privacy concerns relevant to this paper.

Many civilian drones have the capacity to be flown beyond the line of sight of the operator, although to do so is generally illegal.⁵⁰ This can be done through built-in GPS systems that allow a programmed pre-set flight path enabling the drone to target a specific address or location, or else through the use of first-person view technology that transmits the video from a camera mounted on the drone back to the operator.⁵¹ Although Nano-UAVs (drones weighing less than 500g) may lack some of these technologies, even a hand-sized nano-UAV weighing just 50g is capable of carrying a camera and operating with first-person view. The quality of the camera varies between drones, but advanced drones are often outfitted with the highest definition camera on the market that have the capacity to provide real time video streams at a rate of 10 frames a second.⁵² This provides the potential to record far and remote locations or individuals, particularly when coupled with technology that allows the operator to control the camera's pitch quickly and accurately.⁵³

Aside from recording capabilities, many drones also have the power to hover or stabilise, fly autonomous routes, and clock fast speeds allowing the drone to reach new locations quickly.⁵⁴ High-end quadcopters can fly for around 30 minutes, reaching speeds of up to 60 kilometres per hour.⁵⁵ Such fast speeds facilitate particular applications such as drone journalism or search and response efforts and are therefore both advantageous and alarming in the sense that private situations or scenes of accidents can be reached, accessed and broadcasted speedily. Some of these more advanced drones also carry infrared cameras, heat sensors, sensors that detect movement and automated licence plate

⁴⁹ At 156.

⁵⁰ Civil Aviation Rules 2015, r 101.209.

⁵¹ Shelly, above n 45, at 75.

⁵² Electronic Privacy Information Center "Domestic Unmanned Aerial Vehicles (UAVs) and Drones" (2016) <www.epic.org>.

⁵³ Hadyn Green "Drones" (21 April 2016) Consumer NZ <www.consumer.org.nz>.

⁵⁴ Green, above n 53.

⁵⁵ Nick Heath "The long-range drone that can keep up with a car and fly for an hour" (27 May 2015) TechRepublic <www.techrepublic.com>.

readers, although these types of functions are not preconditions for a significant privacy breach to occur.⁵⁶

B A New Privacy Threat

In a pre-computer age, the greatest privacy protections were not legal, but practical, as “traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken”.⁵⁷ Recent years have seen the emergence of many devices that make it easier to monitor and record people’s movements, such as cell phones, CCTV cameras, dash cams, GPS and facial recognition. To an extent the equipment on board drones is already commonplace in the consumer electronics market, as high definition cameras may already be used to capture footage of people without their consent.⁵⁸ This raises the question: how does drone technology present *new* threats to privacy?

Drones may undermine people’s desired inaccess through their ability to capture, and thus jeopardise, multifarious facets of one’s life. Some aspects may include personal data through the monitoring of Wi-Fi emanations or automatic number-plate recognition,⁵⁹ or the privacy of personal communications. However, this paper is primarily concerned with the ability of drones to undermine physical, behavioural, and informational privacy.⁶⁰ Drones can violate these forms of privacy in two ways. First, drones may take one-off images of movements, activities, associations and preferences that may constitute an intrusion or disclose private information about someone.⁶¹ Secondly, drones can undertake constant, persistent surveillance to a degree that former methods of video surveillance were unable to achieve.⁶² Continuous observation and recording, more closely and in high-resolution threatens to capture greater degrees of private information about people that could not be gained through past uses of technology.

⁵⁶ Electronic Privacy Information Center, above n 52.

⁵⁷ *United States v Jones* 565 US __, 132 S Ct 945 (2012) at 12, per Alito J.

⁵⁸ Ann Cavoukian “Privacy and Drones: Unmanned Aerial Vehicles” (August 2012) Information and Privacy Commissioner of Ontario, Canada, Privacy by Design <www.ipc.on.ca> at 10.

⁵⁹ Roger Clarke “The Regulation of Civilian Drones’ Impacts on Behavioural Privacy” (2014) 30 Computer Law and Security Review 286 at 287.

⁶⁰ At 287.

⁶¹ At 287.

⁶² Electronic Privacy Information Center, above n 52.

Drones can be distinguished from other technologies⁶³ by their ability to gather information dynamically from unique vantage points, allowing barriers in the line of sight to be overcome.⁶⁴ Drones can encroach on particular targets or people and take vertical and angled shots.⁶⁵ This allows drones to capture images of places one would expect to be private without the need to trespass, such as bedroom windows or enclosed backyards, but also public areas where one would expect a certain level of privacy, such as being picked out of a large crowd or captured on a reasonably isolated part of a beach.

Drones also often operate covertly or surreptitiously, particularly small nano-UAVs that can appear as insects or birds, giving rise to circumstances where the individual is unaware that they are being recorded.⁶⁶ This limits people's choices in two ways: first, it fails to allow people to convey their unwillingness to be photographed or recorded in the first place, which undermines their power to prevent the interference. Secondly, it does not allow people to alter their behaviour or the information they impart in order to protect their privacy. The revelation of personal harm is missing when the intrusion goes unnoticed, meaning the victim is therefore powerless to seek recourse. If the privacy violation is only realised after the fact, the harm to the individual is likely to be great, as the inability of the individual to alter their actions in light of the observation may have caused the exposure of particularly humiliating or private information or actions. Further, surreptitious photographing or recording is likely to engender vulnerability, violation and mistrust.⁶⁷ In the English case of *Gulati v MGN Ltd*, a combination of people brought a claim after their telephone messages were repeatedly intercepted by journalists over a

⁶³ Anne-Marie Allgrove and Liz Grimwood-Taylor "Privacy in the Drone Era: Applying the Privacy Act to New Technologies" (2016) 13 PrivLB 32 at 34.

⁶⁴ Clarke, above n 59, at 289.

⁶⁵ Cavoukian, above n 58, at 10.

⁶⁶ Clarke, above n 59, at 290.

⁶⁷ N.A. Moreham "Liability for Listening: Why Phone Hacking is an Actionable Breach of Privacy" (2015) 8 Journal of Media Law 155 at 168.

long period of time.⁶⁸ Mann J explained how the plaintiffs felt “violated” and “sickened” by the hacking,⁶⁹ with one saying they felt “persecuted” and “hunted”.⁷⁰

Furthermore, operators are remote from their targets. This detachment from physical reality may weaken the constraints of conscience.⁷¹ Drones give the operator a broader line of sight and they can hone in on particular targets or events without the backlash associated with taking close-range shots with standard cameras. Operating a drone is low-risk, particularly where recreational drones have little identification allowing them to be linked back to their owners. The temptation to push the boundaries of intrusion may become all too strong with increased technological capabilities, coupled with little recourse.

The ease at which drones can capture both one-off images and undertake constant surveillance is demonstrated through recent instances where drones have invaded people’s privacy. The first drone-related complaint in New Zealand, received by the Privacy Commissioner, regarded the use of a drone by Sky TV to film a cricket match.⁷² During the recording of the game the drone flew within 10 metres of the complainant’s apartment that overlooked the cricket venue.⁷³ The complainant was concerned that the drone had captured highly sensitive information about him, however Sky TV maintained that the drone was not filming the entire time it was in the air.⁷⁴ In this case, there was found to be no breach of the Privacy Act 1993 because personal information needed to have been collected and there was no evidence of that here.⁷⁵ This complaint illustrates the ability of drones to intrude into a space inaccessible by others, as well as the way in which drones risk changing the nature of a space from inherently private, where one is likely to have an expectation of privacy considering it is their own home, to a potentially public space. The

⁶⁸ *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch).

⁶⁹ At [32(i)].

⁷⁰ At [405].

⁷¹ Clarke, above n 59, at 290.

⁷² See Privacy Commissioner *Case No 267458* [2015] NZ PrivCmr 6.

⁷³ Privacy Commissioner, above n 72.

⁷⁴ Privacy Commissioner, above n 72.

⁷⁵ Privacy Act 1993, s 6.

privacy torts ought to respond to this increased accessibility, otherwise it would follow that people can no longer expect privacy where they are captured in front of windows within their own home.

In Australia a real-estate agent used a drone to capture aerial photographs of a property and came under scrutiny after the advertising shots captured a woman sunbathing in her backyard.⁷⁶ In the United States, a lawsuit was filed after a resident used a shotgun to bring down a drone, claiming that it was trespassing on his property and thus invading his privacy.⁷⁷ Panic was also caused when a phantom drone, small enough to be confused for a large bird, landed on the lawn of the White House.⁷⁸ These examples demonstrate the variety of privacy threats posed by drones, as well as the panic that has ensued.

IV Developing the Privacy Torts

As established, the law ought to protect against encroachments on privacy by drones, and to an extent the current legal framework does this.⁷⁹ However, there is a void within this framework that might preclude successful claims unless the privacy torts are developed to operate more effectively.

A Current Scope of the Torts

The tort of wrongful publication of private facts was confirmed by the Court of Appeal in *Hosking*, where the Court was concerned with the publication of photos taken of a television presenter's 18-month-old twins being wheeled down a busy street in their

⁷⁶ Natasha Johnson "Topless neighbour's drone picture prompts calls for privacy law overhaul" (17 November 2014) ABCNews <www.abc.net.au>.

⁷⁷ Frost Brown Todd "First Lawsuit to Clarify the Rights of Drone Operators and Property Owners Filed in Federal Court" (January 5, 2016) <www.frostbrowntodd.com>.

⁷⁸ Michael S. Schmidt and Michael D. Shear "A Drone, Too Small For Radar to Detect, Rattles the White House" (26 January 2015) New York Times <www.nytimes.com>.

⁷⁹ The Civil Aviation Rules 2015, r 101.201-101.215 address issues of safety by regulating the operation of drones. The Privacy Act 1993, s 6 concerns the collection, storing and use of personal information by agencies (however the Act does not apply if someone is collecting information in their personal capacity). The Broadcasting Act 1989 provides that broadcasters must observe standards that are consistent with the privacy of the individual. The Crimes Act 1961, s 216H applies where drones are used to make covert intimate recordings of people without their consent or knowledge, in a place where they would have a reasonable expectation of privacy. The Summary Offences Act 1981, s 30 might apply where a drone is used to peer into someone's home and record activity within.

pushchair.⁸⁰ Although there was found to be no breach of privacy, the majority of the Court established a two-pronged test for breaches of informational privacy:⁸¹

- (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.

In addition, there is an available defence justifying publication where there is a legitimate public concern in the facts published. This concern will be balanced against the harm likely to be caused by the breach of privacy.⁸² The burden for proving the defence is on the defendant, and it is not available where the matter is of no more than general interest or titillation, or gives rise to curiosity.⁸³

This tort does not extend to the mere acquisition of information, nor situations where a defendant merely watches, records or physically encroaches on a claimant.⁸⁴ Accordingly a claim cannot be brought under the *Hosking* tort in instances where a drone is used to record or film a person, but rather where widespread publicity of the information obtained through the recording has also occurred.

Fittingly, the High Court in *C v Holland* extended the common law to establish a second privacy tort covering situations of unwanted physical access.⁸⁵ *Holland* concerned the secret video recording by Holland of his flatmate's girlfriend through a hole in the ceiling while she showered.⁸⁶ The video was kept on his laptop, but not distributed or

⁸⁰ *Hosking v Runting*, above n 2, at [9]-[11].

⁸¹ At [117].

⁸² At [134].

⁸³ Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy, Stage 3* (NZLC IP14, 2009) at 22.

⁸⁴ N.A. Moreham "A Conceptual Framework for the New Zealand Tort of Intrusion" (2016) 47 VUWLR (forthcoming) at 6.

⁸⁵ *C v Holland*, above n 25.

⁸⁶ At [2].

published.⁸⁷ Whata J held that the establishment of the tort of intrusion into seclusion was “entirely compatible with, and a logical adjunct to, the *Hosking* tort”. As such, Whata J outlined the following elements to the tort of intrusion into seclusion:⁸⁸

- (1) an intentional and unauthorised intrusion;
- (2) into seclusion (namely intimate personal activity, space or affairs);
- (3) involving infringement of a reasonable expectation of privacy; and
- (4) that is highly offensive to a reasonable person.

The latter two elements of Whata J’s formulation are taken directly from the *Hosking* test.⁸⁹ A legitimate public concern in the information again provides a defence to any claim.⁹⁰

B Reasonable Expectation of Privacy

The test of a reasonable expectation of privacy is more appropriate than alternative tests, despite criticism for its incoherence and uncertainty.⁹¹ Other tests, such as examining whether the information is clearly private or attempting to list categories of private information are bound to fail, as the desires of people for the privacy of different types of information vary.⁹² Moreover, there is necessarily a sliding scale of trivial and serious information within any category.⁹³ For example, to regard medical information as inherently private would compel the courts to conclude that disclosure that an individual suffers a cold is a breach of privacy.⁹⁴

⁸⁷ At [2].

⁸⁸ At [94].

⁸⁹ Thomas Levy McKenzie “The New Intrusion Tort: The News Media Exposed?” (2014) 45 VUWLR 79 at 84.

⁹⁰ *C v Holland*, above n 25, at [96].

⁹¹ See generally Eric Barendt “‘A Reasonable Expectation of Privacy’: A Coherent or Redundant Concept?” in Andrew T. Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 96.

⁹² At 105.

⁹³ At 105.

⁹⁴ Moreham, above n 5, at 641-2.

Privacy claims are therefore not endangered by the test itself, but rather the way in which the courts approach this test. It is proposed that the most effective development of the torts will derive from undertaking both a normative and multifaceted approach.

1 Normative approach

The use of the ‘reasonable person’ and his or her expectations needs to afford a normative consideration of whether any given privacy intrusion by a drone is worthy of protection. As Moreham emphasises, the courts erroneously focus liability on whether privacy is *likely* to be respected on the facts, rather on whether it *ought* to be respected.⁹⁵ The Supreme Court of California’s decision of *Shulman v Group W Productions Ltd* is indicative of this concern.⁹⁶ The case concerned a woman who was filmed being attended to by paramedics on a highway following a serious accident.⁹⁷ The Court held that the claimant had no reasonable expectation of privacy because it is expected or at least usual practice for journalists to record scenes of accidents.⁹⁸ This decision tacitly emphasises that privacy applies in systemic ways throughout society in accordance with the values and norms of that society.⁹⁹

The United States case of *United States v Jones* was concerned with whether the installation of a GPS tracking device to monitor the movement of a vehicle constituted a search under the Fourth Amendment.¹⁰⁰ Alito J (majority) challenged the notion that the reasonable person has a “well-developed and stable set of privacy expectations”, stating that technological change may produce significant changes in popular attitudes.¹⁰¹ He considered that new technology provides increased security and convenience at the expense of privacy, and many people may find that trade off worthwhile, or at least come to accept this diminution of privacy as inevitable.¹⁰²

⁹⁵ At 647.

⁹⁶ *Shulman v Group W Productions Ltd* 955 P 2d 469 (Cal 1998).

⁹⁷ *Shulman v Group W Productions Ltd*, above n 96.

⁹⁸ At 864.

⁹⁹ Robert L. McArthur “Reasonable Expectations of Privacy” (2001) 3 Ethics and Information Technology 123 at 125.

¹⁰⁰ *United States v Jones*, above n 57.

¹⁰¹ At 10, per Alito J

¹⁰² At 10, per Alito J.

While it is recognised that societal standards influence people’s expectations of privacy, the judgments in *Shulman* and *Jones* represent a descriptive rather than a normative analysis that the New Zealand courts ought not to follow. Drones push to redefine the expectations that people have about their own privacy. If the courts rely purely on societal expectations, and are unfastened in their view of what those expectations might be, we risk losing the very protection that the torts set out to achieve. Instead of further limiting the boundaries in which one could expect privacy due to advances in technology, drones ought to act as the visceral jolt society needs to drag privacy law up to date and restore normative models of privacy violations.¹⁰³ Retaining normative notions of privacy when analysing one’s reasonable expectation is paramount in light of the threats posed by drones.

2 *Multifaceted approach*

Drones necessitate a variety of factors to be considered under the test, so that the focus is on whether the ‘zone’ of intimacy falls within the scope of private or public life, rather than the precise nature of the location where the activity occurred.¹⁰⁴ The tort of intrusion into seclusion focuses the inquiry on whether there is a reasonable expectation of privacy in the intimate personal activity, space or affairs,¹⁰⁵ whilst the *Hosking* tort looks to the information or material.¹⁰⁶ Despite this distinction, the courts ought to consider similar factors under their approach.

¹⁰³ Calo, above n 1, at 29.

¹⁰⁴ *Von Hannover v Germany* [2004] ECHR 294 at [50] and [64].

¹⁰⁵ William Fussey “Applying and Developing the Intrusion into Seclusion Tort in New Zealand” (LLB (Masters) Thesis, Victoria University of Wellington, 2015) at 36.

¹⁰⁶ According to Gault P and Blanchard J, there must be “private facts” in which there is a reasonable expectation of privacy. Tipping J instead observed that the necessary expectation of privacy could arise from the nature of the information or “material”, or the circumstances in which the defendant came into possession of it, or both.

(a) Location

Conventionally privacy has been inextricably linked to private spaces,¹⁰⁷ but drones alter the rigid dichotomy between public and private so that locations should no longer be branded accordingly. Although the most secluded places or interactions, such as in the private home or bathroom, will more easily satisfy the test, drones pervade barriers that would usually determine the nature of a location. In the wake of drones, spheres of privacy are better assessed by reference to physical, behavioural and normative barriers.¹⁰⁸ Physical barriers include things such as walls, doors, hedges and safes,¹⁰⁹ meaning that private locations closed off by virtue of their physical barriers present the most obvious signs of a private space. Not all intrusions or access to a person will necessarily breach a physical barrier.¹¹⁰ Behavioural barriers are verbal or non-verbal communication that convey an individual's desired inaccess, and a normative barrier is derived from "the normal rules of social interaction", being a societal expectation that a person does not want their privacy infringed.¹¹¹

The analysis of the types of barriers that might represent a private space is relevant to drones for the following reasons. First, there may be physical barriers in what would ordinarily be deemed public spaces. For example, someone may shelter behind a tree to get changed. The act of hiding behind this physical barrier changes the nature of the space. Drones have greater ability to pervade these physical barriers, allowing privacy violations to occur with ease. Furthermore, behavioural and normative barriers ought to garner the same amount of respect yet these barriers are harder to identify by drone operators who are at a distance from the subject. An individual may have the opportunity to convey to others on a street through behaviour or communication that they are undertaking something private. However, they will not have that same opportunity when a

¹⁰⁷ Patricia Sanchez Abril "Recasting Privacy Torts in a Spaceless World" (2007) 21 *Harvard Journal of Law and Technology* 1 at 3.

¹⁰⁸ Kirsty Hughes "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75 *MLR* 806 at 809.

¹⁰⁹ At 812.

¹¹⁰ Fussey, above n 105, at 17.

¹¹¹ Hughes, above n 108, at 812.

drone is capturing the moment from far away, potentially surreptitiously. Here the courts ought to recognise that some actions may intrude into a 'private space' despite the actual locality of the matter. The courts should therefore inquire as to what barriers have been, or would have been, established by the individual had they known about the presence of the drone or been given the opportunity to communicate with the drone operator in the first instance.

This approach to location is more satisfactory because individuals undertake their own subjective evaluation of privacy risks in any given situation and adapt their behaviour accordingly. In a traditionally 'public' place people have the ability to choose how much or how little they reveal to others within their proximity.¹¹² Where an individual is in a place that is theoretically public but is sufficiently remote so as to have an element of isolation,¹¹³ they are likely to make fewer self-preservation efforts as if the space was more akin to a private space rather than a public one.

Another reason why the courts should avoid a bright line distinction between public and private places is because those that observe an individual are able to disseminate information about them to a broader audience than the one that individual was initially exposed to.¹¹⁴ This is important because an individual will tailor their actions to the limited number of people who might observe them within that particular space at that particular time.¹¹⁵ The Court in *Peck v United Kingdom* was concerned with the publication of CCTV footage that captured the applicant walking through the Brentwood mall at midnight and his suicide attempt within that time.¹¹⁶ Although passers-by could have witnessed the events that were later publicised, the Court considered that the relevant moment was viewed to an extent that far exceeded any exposure to people present at the scene and to a degree far surpassing what the plaintiff could have foreseen when walking

¹¹² N.A. Moreham "Privacy in Public Places" (2006) 65 CLJ 606 at 617.

¹¹³ At 622.

¹¹⁴ At 618.

¹¹⁵ At 619.

¹¹⁶ *Peck v United Kingdom* (2003) 36 EHRR 41.

in that public space.¹¹⁷ Although it was CCTV footage rather than a drone that captured the relevant moments in *Peck*, an analogy can be drawn on the basis that the plaintiff was completely unaware of the recording taking place and therefore could not have foreseen the potential exposure, as is likely to be the case where drones record surreptitiously.

Location should still be a factor relevant to the determination of a reasonable expectation of privacy because specific locations, such as the home, will be conceptually linked with intimacy and personal privacy.¹¹⁸ Still, the courts should perceive location on a sliding scale by considering the types of barriers that one has put up. These barriers ought to define the nature of the space more than traditional notions of location do.

(b) Method of intrusion or acquisition of the information

The method of intrusion, or manner in which the information is obtained, becomes more relevant where drones are concerned. The need to use surreptitious means, or photograph from long distances at unparalleled vantage points, to intrude upon the plaintiff's activity is indicative that the plaintiff did not intend the activity to be public in the first place.¹¹⁹ The more intrusive the method, the more the defendant has had to work to pervade any type of obstacle the plaintiff has put up in order to avoid detection.

This approach is a logical extension of existing observations within the courts. The reference to 'intimate personal activity' within the formulation of the intrusion tort acknowledges the need to establish intrusion into matters that most directly impinge on personal autonomy.¹²⁰ In the United States, Powell J (dissenting) pointed out in the decision of *California v Ciraolo* that an emphasis on physical intrusion "provides no real protection against surveillance techniques made possible through technology".¹²¹ The courts recognise that the more isolated or distant an activity is, the larger the reasonable

¹¹⁷ At 739.

¹¹⁸ Richard G. Wilkins "Defining the Reasonable Expectation of Privacy: An Emerging Tripartite Analysis" (1987) 40 Vand L Rev 1077 at 1112.

¹¹⁹ McKenzie, above n 89, at 94.

¹²⁰ *C v Holland*, above n 25, at [95].

¹²¹ *California v Ciraolo* 476 US 207 (Cal 1986) at 218.

expectation of privacy, particularly where what is observed can only be seen with the aid of technology.¹²²

In *Hosking* Gault P and Blanchard J commented “the intrusiveness of the long-range lens and listening devices...are the factors in modern society of which the law must take account”.¹²³ Tipping J noted that the circumstances in which the defendant came into possession of the information or material may give rise to the necessary expectation of privacy.¹²⁴ In the United Kingdom the method of acquisition has also been considered relevant. In *Hellewell v Chief Constable of Derbyshire* it was held that the use of a telephoto lens may give rise to liability.¹²⁵ In *Peck* it was relevant that the plaintiff was filmed surreptitiously.¹²⁶ Likewise in *Campbell*, Lord Hoffman went so far as to say that the publication of a photograph taken by intrusion into a private place, for example by a long-range lens, may in itself be such an infringement of an expectation of privacy even if there is nothing inherently embarrassing in the photograph itself.¹²⁷ However, it must be noted that Baroness Hale disagreed, as she was of the opinion that the activity itself must be private and saw the mere fact of covert photography as insufficient to make the information confidential.¹²⁸

News outlets are a prime example of a user of drones that will capitalise on the speed and ease at which they can access events or people, and through such invasive means will disclose information otherwise inaccessible. Such scenarios are far more intrusive than people observing loud conversations that occur between others on the street, or even a photographer capturing a photo from short-range of someone going about their daily activities completely in the open, such as in *Hosking*. Individuals are likely to be unaware they are being recorded when devices such as drones are used to record from far distances

¹²² Fussey, above n 105, at 75.

¹²³ *Hosking v Runtig*, above n 2, at [109].

¹²⁴ At [249].

¹²⁵ *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, [1995] 4 All ER 473.

¹²⁶ *Peck v United Kingdom*, above n 116, at 304.

¹²⁷ *Campbell v Mirror Group Newspapers Ltd*, above n 43, at [75].

¹²⁸ At [154].

with long lens cameras, meaning that people are not given the chance to limit their exposure, alter their actions or express their lack of consent.

Commentators have argued that the method of intrusion should not in itself give rise to a reasonable expectation of privacy,¹²⁹ but the invasiveness of drones should warrant heightened protection as activities, places or events in which people would normally expect to be private will be compromised. However, there may be circumstances in which a drone captures information that could also have been, or was, obtained from on the ground or captured by a standard camera. Here the mere fact that a drone was used should not automatically point towards a more invasive method of acquirement and thus a reasonable expectation of privacy. The courts must consider whether the unique functions of the drone have provided it with the greater capabilities, such that the information would not be ordinarily accessible.

(c) Depiction of the information

As drones gain popularity, an increased amount of people's lives will be captured in images and thus permanently recorded. The courts have distinguished between photographs and descriptions so that the publication of a photograph or footage can be actionable even where the publication of the description providing the same type of information is not.¹³⁰ In *Douglas v Hello!* Keene LJ said that the photographs conveyed information to the public that was not otherwise obtainable, namely what the events and its participants looked like.¹³¹ One cannot treat a photograph as a means of conveying factual information because the photograph is a more vivid form,¹³² and thus provides more than a verbal description of it.¹³³

¹²⁹ See Raymond Wacks *Privacy and Press Freedom* (Blackstone Press, London, 1995) at 137.

¹³⁰ Moreham, above n 112, at 614.

¹³¹ *Douglas v Hello! (No. 1)* [2001] QB 967, [2001] WLR 992 at [165].

¹³² *Campbell v Mirror Group Newspapers Ltd*, above n 43, at [72].

¹³³ *Douglas v Hello! (No. 3)* [2005] EWCA Civ 595, [2005] 3 WLR 881 at [106].

Moreover, the mere fact that a drone has captured a photograph of someone within a public place is not necessarily allowable on the sole ground that others in that location could have been exposed to the information themselves.¹³⁴ As noted by Randerson J, there is a distinction between “the fleeting glimpse of the children which passers-by may have had in the street and the publication of a semi-permanent record”.¹³⁵ In *Andrews v Television New Zealand Ltd* it was observed that although a car crash occurred in a public place, the footage that was recorded and later televised went beyond mere observation of the scene and was prolonged and thus gave rise to a reasonable expectation of privacy.¹³⁶ In *Television New Zealand v Rogers* a video that contained public facts about a confession to a murder could still give rise to an expectation of privacy due to the manner and circumstances in which the confession was made.¹³⁷ It was the enhancement given to the material by showing it live and the graphically intimate and personal details of the plaintiff’s personality and demeanour that meant the video confession was not precluded from constituting a private fact.¹³⁸ The decisions in both *Andrews* and *Rogers* appear to be largely based on the recognition that the plaintiffs were made more accessible than they otherwise would have liked because the publicity given to the footage went beyond mere observation of the scene, or portrayed more than the facts already disclosed to the public.¹³⁹

The fact that imagery portrays more than the written word acts as an incentive for news outlets and laypeople to use drones to capture images and videos of scenes rather than simply report on them. If photographs that depict no more than passers-by could have observed on the day could potentially justify privacy protection, it follows that the capturing of images from unique vantage points otherwise unobtainable is likely to give rise to an expectation of privacy. The publication of continuous footage, such as in

¹³⁴ Stacey Lulham “What is, and What Should Be, the Extent of New Zealand’s New Tort of Breach of Privacy?” (2005) 11 Canterbury L Rev 91 at 102.

¹³⁵ *Hosking v Runting* [2003] 3 NZLR 385 (HC) at [139].

¹³⁶ *Andrews v Television New Zealand Ltd* [2009] 1 NZLR 220 (HC) at [65].

¹³⁷ *Rogers v Television New Zealand Ltd* [2007] NZSC 91, [2008] 2 NZLR 277 at [68] per Tipping J.

¹³⁸ At [68] per Tipping J and [101] per McGrath J.

¹³⁹ Ursula Cheer “The Future of Privacy: Recent Legal Developments in New Zealand” (2007) 13 Canterbury L Rev 169 at 176.

Andrews, would give rise to a greater expectation of privacy than a single image. Where one-off images may not violate a person's privacy, the total sum of sequences of images might,¹⁴⁰ as a "pattern of life" emerges whereby important aspects of people can be revealed through their gestures, posture, attitude towards others and even speech.¹⁴¹

However, it does not follow that there will be no reasonable expectation of privacy where drones capture information through photographing or recording, but only the text describing what was obtained is published. The text will almost always disclose less information than the actual imagery but would be for the courts consider all the factors relevant to the particular case. Potentially the general inaccessibility of the activity or information could give rise to a reasonable expectation of privacy even where only the textual description is disclosed.

(d) Nature of the activity or information

The courts ought to adapt the current approach to establishing private facts or activities in light of the ability of drones to access and observe the most intimate activities or information. As understood in *Hosking*, certain kinds of information may be easily identified as private, such as information relating to health, personal relationships, or finances.¹⁴² Similarly in *Murray v Express Newspapers plc* it was said that routine acts such as a visit to the shop or a ride on the bus should not attract a reasonable expectation of privacy.¹⁴³ Moreham explains that taking a photograph in a public place "should be legally actionable if the person photographed is involuntarily having an intimate or traumatic experience".¹⁴⁴ The acknowledgement that the most unrestricted and public kinds of activities will not warrant protection ought not to change where a drone is involved. However, what constitutes private information where it is less obvious is

¹⁴⁰ Andrew Jay McClurg "Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places" (1995) 73 NC L Rev 987 at 1043.

¹⁴¹ At 1043-1044.

¹⁴² *Hosking v Runtig*, above n 2, at [119], citing *Australian Broadcasting Corporation v Lenah Game Meats* [2001] HCA 63, (2001) 185 ALR 1 at [42].

¹⁴³ *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch 481 at [66].

¹⁴⁴ Moreham, above n 112, at 634.

inherently subjective and the current approach requires judges to make value judgments about the objective offensiveness of the subject matter.¹⁴⁵

The advent of drones should see the courts look less to the subject matter in isolation, but look instead to both the objective perceptions regarding information or an activity, and also what the plaintiff has communicated in terms of their subjective attitude to those facts. People have differing subjective ideas about what information or activities they wish to protect, as subject matter is related to a sphere of individual action or emotional sanctum.¹⁴⁶ It is untenable to allow drone operators to pervade or ignore subjective desires of privacy simply because the activity or information is not objectively private. To do so would undermine the plaintiff's dignity and control over that activity or information. Subjective expectations of individuals regarding what information they wish others to know about their life may also become indicative of objective expectations.¹⁴⁷ Thus a drone capturing a couple kissing in a crowd at a sports game is likely to be an activity warranting less protection than if the drone had captured them kissing within the privacy of their own home, or in an otherwise isolated part of a park or beach. In an intrusion context, minimal information may be obtained however the nature of the activity might be subjectively personal.¹⁴⁸

Moreover, the imprecision of what might be determined private information is due to the reliance on prevailing standards of taste and decency within a society.¹⁴⁹ Attitudes to infidelity, divorce, mental illness and sexual relations change over time.¹⁵⁰ A community will never be homogenous in terms of its views due to the plurality of ages, religions, cultures and political beliefs.¹⁵¹

¹⁴⁵ Melissa Waterfield "Now You See It, Now You Don't: The Case for a Tort of Infringement of Privacy in New Zealand" (2004) 10 *Canterbury L Rev* 182 at 4.

¹⁴⁶ Abril, above n 107, at 20.

¹⁴⁷ Fussey, above n 105, at 91.

¹⁴⁸ At 86.

¹⁴⁹ Waterfield, above n 145, at 4.

¹⁵⁰ At 4.

¹⁵¹ At 4.

Taking a contextual and multifaceted approach to the test means that where the place and the intrusiveness give rise to a high reasonable expectation of privacy, the nature of the activity or information should become less of a concern.

C Highly Offensive

The purpose of the highly offensive test is to ensure that the “shrinking soul” who is unusually sensitive about publicity is not protected.¹⁵² However, the test is of little analytical significance and may undermine potentially successful claims where breaches of privacy by drones occur. The test entails a value judgment for which it is difficult to provide clear reasons.¹⁵³ The test is an objective determination of whether the publication or intrusion is offensive “causing real hurt or harm”.¹⁵⁴ Courts may examine the extent and nature of breach with reference to factors such as the degree of the intrusion, the circumstances surrounding the intrusion or observation, and the expectations of the person whose privacy is invaded.¹⁵⁵

The lack of analytical significance is ostensible because, as stated by Tipping J in *Hosking*, in most cases a reasonable expectation of privacy will arise when publication (or intrusion) would cause a high degree of offence, and therefore this second criterion is implicit in the first.¹⁵⁶ Randerson J echoed this view by commenting that instead of being a separate requirement, the offensiveness test should be used to help identify what might be regarded as private information.¹⁵⁷ This view is consistent with that of the Court in *Campbell* where it was largely agreed that the stricter offensiveness test should be used with care, and perhaps used only in borderline cases.¹⁵⁸ Factors relevant to the privacy risks associated with drones, such as intrusiveness, have already been dealt with and the highly offensive test is therefore redundant.

¹⁵² William L Prosser “Privacy” (1960) 48 CLR 383 at 397.

¹⁵³ N.A. Moreham “Private Matters: A Review of the Broadcasting Standards Authority” (New Zealand Broadcasting Standards Authority, 2009) at 15.

¹⁵⁴ *Hosking v Runtig*, above n 2, at [126].

¹⁵⁵ *Miller v National Broadcasting Company* 187 Cal App 1463 (Cal 1987) at 679.

¹⁵⁶ *Hosking v Runtig*, above n 2, at [256].

¹⁵⁷ *Hosking v Runtig*, above n 135, at [161].

¹⁵⁸ *Campbell v Mirror Group Newspapers Ltd*, above n 43, at [22], [94], [136] and [166].

The ‘offensive’ element is difficult to apply, which could instead result in the consideration of very separate factors under the highly offensive test. For example, in *P v D* it was suggested that society’s likely reaction to the disclosure is relevant, as an adverse reaction would indicate that the plaintiff would likely be offended.¹⁵⁹ This could have the undesirable effect of undermining factors significant to drones, considered at the reasonable expectation of privacy stage. In *Andrews*, the plaintiff’s claim failed because there was nothing included in the footage that portrayed them in a negative way.¹⁶⁰ This failed to recognise that the plaintiffs were filmed in a very intimate situation for a long period of time, and the publication of their exchanges of words and vulnerabilities caused them real humiliation when the documentary was broadcasted.¹⁶¹ Taken in its strictest sense, requiring proof of real hurt or harm bears the risk of “obscuring the fact that all privacy interferences undermine the plaintiff’s dignity”.¹⁶² The courts risk pigeonholing the circumstances in which a plaintiff may suffer real hurt or harm to where the information is inherently offensive or private, judged once again by objective moral standards. It risks setting the bar too high, especially in cases where the countervailing free speech claim is weak compared to the privacy infringement.¹⁶³ By adding an additional hurdle to recovery, the highly offensive test risks failing to protect plaintiffs even when drones severely undermine their dignity.¹⁶⁴

D Mental Element

Drones are controlled at a distance, which gives rise to practical difficulties associated with proving the mental requirement of the torts. For an actionable intrusion, there needs to be an affirmative, intentional act rather than an unwitting or careless intrusion, such as innocently walking in on a friend in the bathroom.¹⁶⁵ As to the *Hosking* tort, it is less clear what mental element is required, if any. Arguably there is the requirement of an intention

¹⁵⁹ *P v D* [2000] 2 NZLR 591 (HC) at 601.

¹⁶⁰ *Andrews v Television New Zealand Ltd*, above n 136, at [68]-[69].

¹⁶¹ McKenzie, above n 89, at 97.

¹⁶² Moreham, above n 6, at 240.

¹⁶³ Chris Hunt “Breach of Privacy as a Tort” [2014] 8 NZLJ 286 at 288, citing *Hosking v Runtig*, above n 2, at [256].

¹⁶⁴ McKenzie, above n 89, at 97.

¹⁶⁵ *C v Holland*, above n 25, at [95].

to publish the information acquired by a drone and, for the most part, publication is hardly ever anything but an intentional act, especially where the media is concerned.¹⁶⁶

It is easier for a drone operator to argue that they did not intend the drone to intrude into a secluded space when, for example, they captured images of a person from outside their window, than it would for a peeping Tom to argue they did not intend to peep through a window into someone's bathroom. A lower threshold of recklessness may therefore be more appropriate in the drone context, as it would prevent defendants from making dishonest arguments such as they merely wanted to capture scenery or the information was accidentally caught within the background of a shot. Aspects of the law implicitly support this approach. Under the Crimes Act 1961 it is an offence to make an intimate visual recording intentionally or recklessly.¹⁶⁷ In the United Kingdom the Data Protection Act 1998 creates an offence of obtaining, disclosing or procuring the disclosure of personal information knowingly or recklessly, without the consent of the organisation holding the information.¹⁶⁸ These provisions cover situations analogous to privacy breaches caused by drones, showing the viability of a lower recklessness standard.

However, imposing recklessness as the qualifying fault standard risks broadening the scope of liability too far. In *Wainwright and other v Home Office* Lord Hoffman distinguished between wandering carelessly into the wrong hotel bedroom and hiding in the wardrobe to take photographs.¹⁶⁹ It follows that the objective of the defendant is likely to be relevant to the extent of the intrusion or publication, and there is obviously a higher degree of moral culpability where there is subjective intention. In the United States, the defendant's intent has been considered relevant, as evidence of outrageous, intentional and systematic campaigns to harass or embarrass have been held to indicate greater invasions of privacy.¹⁷⁰

¹⁶⁶ Law Commission, above n 83, at 155.

¹⁶⁷ Crimes Act 1961, s 216H.

¹⁶⁸ Data Protection Act 1998 (UK), s 55.

¹⁶⁹ *Wainwright and another v Home Office* [2003] UKHL 53 (HL), [2004] 2 AC 406 at [51].

¹⁷⁰ Abril, above n 107, at 36.

To an extent, the fear of broadening the scope of liability too far is mitigated by the reasonable expectation of privacy and highly offensive tests. Where a drone operator has been reckless, it is unlikely that the activity or information will be so severe as to satisfy these two tests. What a lower fault standard would do, however, is ensure that an operator cannot use the excuse of lack of intention where there has been a clear and harmful privacy violation. The courts will need to consider how to approach this practical implication, and whether it warrants a reconsideration of the necessary mental requirement, or an elimination of it altogether.

V Conclusion

In their current state, the New Zealand privacy torts are inapt to deal with unprecedented privacy violations effectuated by drone operators. Although the purpose of the torts is not to provide freedom from all unwanted privacy violations,¹⁷¹ the unique capabilities of drones may provide for more serious encroachments on people's privacy of the type that warrant protection by the torts.

The torts are sufficiently flexible to allow for the development of a clearer framework appropriate to drones. This paper has discussed how the courts ought to use a normative and multifaceted approach to establishing a reasonable expectation of privacy. The factors to account for a not wholly new, but should be emphasised and considered differently in light of the distinct context of drones. The highly offensive test ought to be reconsidered as it adds little to the substance of the torts, but more disconcertingly the test risks completely undermining privacy claims within the context of drones where the courts focus too narrowly on the nature of the activity or information in determining overall offensiveness. Finally, the courts need to establish a clearer and more practical mental requirement for the torts that ensures liability is not unduly found, but still protects plaintiffs from loopholes that drone operators may easily rely on.

¹⁷¹ Stephen Dodd "Tortious Intrusions Upon Solitude and Seclusion: A Report From New Zealand" (2015) 27 SAclJ 731 at 731.

One's interest maintaining solitude or protecting private information has to be set against another's interest in the freedom to speak, as well as the importance of publication of information that is of legitimate concern to the public in a free and democratic society.¹⁷² This paper does not attempt to undermine that, nor the ability of people to embrace new technologies, but instead illustrates the need for the development of the privacy torts to best balance people's right to privacy against these other liberties.

¹⁷² McKenzie, above n 89, at 80.

Word Count

The text of this paper (including substantive footnotes, excluding cover page, contents, footnotes and bibliography) consists of 7, 991 words.

VI Bibliography

A Cases

1 New Zealand

Andrews v Television New Zealand Ltd [2009] 1 NZLR 220 (HC).

Brooker v Police [2007] NZSC 30, [2007] 3 NZLR 91.

C v Holland [2012] NZHC 2155, [2012] 3 NZLR 672.

P v D [2000] 2 NZLR 591 (HC).

Hosking v Runting [2003] 3 NZLR 385 (HC).

Hosking v Runting [2005] 1 NZLR 1 (CA).

Rogers v Television New Zealand Ltd [2007] NZSC 91, [2008] 2 NZLR 277.

Tucker v News Media Ownership Ltd HC Wellington CP477/86, 22 October 1986.

Tucker v News Media Ownership Ltd [1986] 2 NZLR 716 (HC).

2 Australia

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd [2001] HCA 63, (2001) 185 ALR 1.

3 United Kingdom

Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22, [2004] 2 AC 457.

Douglas v Hello! (No. 1) [2001] QB 967, [2001] WLR 992.

Douglas v Hello! (No. 3) [2005] EWCA Civ 595, [2005] 3 WLR 881.

Gulati v MGN Ltd [2015] EWHC 1482 (Ch).

Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804, [1995] 4 All ER 473.

Murray v Express Newspapers plc [2008] EWCA Civ 446, [2009] Ch 481.

Peck v United Kingdom (2003) 36 EHRR 41.

Wainwright v Home Office [2003] UKHL 53 (HL), [2004] 2 AC 406.

4 *United States*

California v Ciraolo 476 US 207 (Cal 1986).

Hamberger v Eastman 206 A.2d 239 (N.H 1964).

Miller v National Broadcasting Company 187 Cal App 1463 (Cal 1987).

Shulman v W Productions Ltd 955 P 2d 469 (Cal 1998).

United States v Jones 565 US __, 132 S.Ct. 945 (2012).

5 *Other*

Von Hannover v Germany [2004] ECHR 294.

B *Legislation*

1 *New Zealand*

Broadcasting Act 1989.

Crimes Act 1961.

Privacy Act 1993.

Summary Offences Act 1981.

Civil Aviation Rules 2015.

2 *United Kingdom*

Data Protection Act 1998.

C *Books and Chapters in Books*

Alan F. Westin *Privacy and Freedom* (Atheneum, New York, 1967).

Daniel J. Solove *Understanding Privacy* (Harvard University Press, Cambridge, 2008).

Eric Barendt “‘A reasonable expectation of privacy’: A coherent or redundant concept?” in Andrew T. Kenyon (ed) *Comparative Defamation and Privacy Law* (Cambridge University Press, Cambridge, 2016) 96.

Michel Foucault *Discipline and Punish: The Birth of the Prison* (2nd ed, Vintage Books, New York, 1975).

N.A. Moreham “Privacy Rights” in Mark Warby, Nicole Moreham and Iain Christie (eds) *Tugendhat & Christie: The Law of Privacy and the Media* (2nd ed, Oxford University Press, Oxford, 2011) 59.

N.A. Moreham “Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort” in Jeremy Finn and Stephen Todd (eds) *Law, Liberty, Legislation* (LexisNexis, Wellington, 2008) 231.

S. Benn “Privacy, Freedom, and Respect for Persons” in J. Roland Pennock and John W. Chapman (eds) *Privacy: NOMOS XIII* (Atherton Press, New York, 1971) 1.

Raymond Wacks *Privacy and Press Freedom* (Blackstone Press, London, 1995).

D Journal Articles

Andrew Jay McClurg “Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places” (1995) 73 NC L Rev 987.

Andrew V. Shelly “Application of New Zealand Privacy Law to Drones” (2016) 12 Policy Quarterly 73.

Anne-Marie Allgrove and Liz Grimwood-Taylor “Privacy in the Drone Era: Applying the Privacy Act to New Technologies” (2016) 13 PrivLB 32.

Charles Fried “Privacy” (1968) 77 Yale LJ 475.

Chris Hunt “Breach of Privacy as a Tort” [2014] 8 NZLJ 286.

Daniel J. Solove “A Taxonomy of Privacy” (2006) 154 U Pa L Rev 477.

James Rachels “Why Privacy is Important” (1975) 4 Philosophy and Public Affairs 323.

Jerry Berman and Paula Bruening “Is Privacy Still Possible in the Twenty-First Century?” (2001) 68 Social Research 306.

Julie E. Cohen “What Privacy is For” (2013) 126 Harv L Rev 1.

Kirsty Hughes “A Behavioural Understanding of Privacy and its Implications for Privacy Law” (2012) 75 MLR 806.

Melissa Waterfield “Now You See It, Now You Don’t: The Case for a Tort of Infringement of Privacy in New Zealand” (2004) 10 Canterbury L Rev 182.

M. Ryan Calo “The Boundaries of Privacy Harm” (2011) 86 Ind LJ 1131.

M. Ryan Calo “The Drone as Privacy Catalyst” (2011) 64 Stan L Rev 29.

M. Ryan Calo “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship” (2010) 114 Penn St L Rev 809.

N.A. Moreham “A Conceptual Framework for the New Zealand Tort of Intrusion” (2016) 47 VUWLR (forthcoming).

N.A. Moreham “Beyond Information: Physical Privacy in English Law” (2014) 73 CLJ 350.

N.A. Moreham “Liability for Listening: Why Phone Hacking is an Actionable Breach of Privacy” (2015) 8 Journal of Media Law 155.

N.A. Moreham “Privacy in Public Places” (2006) 65 CLJ 606.

N.A. Moreham “Private Matters: A Review of the Broadcasting Standards Authority” (New Zealand Broadcasting Standards Authority, 2009).

N.A. Moreham “The Protection of Privacy in English Common Law: a doctrinal and theoretical analysis” (2005) 121 LQR 628.

Patricia Sanchez Abril “Recasting Privacy Torts in a Spaceless World” (2007) 21 Harvard Journal of Law and Technology 1.

Richard G. Wilkins “Defining the Reasonable Expectation of Privacy: An Emerging Tripartite Analysis” (1987) 40 Vand L Rev 1077.

Robert C. Post “Rereading Warren & Brandeis: Privacy, Property and Appropriation” (1991) 41 Case W Res L Rev 647.

Robert C. Post “Three Concepts of Privacy” (2001) 89 Geo LJ 2087.

Robert L. McArthur “Reasonable Expectations of Privacy” (2001) 3 Ethics and Information Technology 123.

Roger Clarke “The Regulation of Civilian Drones’ Impacts on Behavioural Privacy” (2014) 30 Computer Law and Security Review 286.

Ruth Gavison “Privacy and the Limits of Law” (1980) 89 Yale LJ 421.

Samuel D. Warren and Lewis D. Brandeis “The Right to Privacy” (1890) 4 Harv L Rev 193.

Sarah A Hinchliffe “Drones - a ‘Serious’ Invasion of Privacy in the Digital Era?” (2014) 11 PrivLB 155.

S. I. Benn “Freedom, Autonomy and the Concept of a Person” (1975-1976) 76 Proceedings of the Aristocratic Society 109.

Stacey Lulham “What is, and What Should Be, the Extent of New Zealand’s New Tort of Breach of Privacy?” (2005) 11 Canterbury L Rev 91.

Stephen Dodd “Tortious Intrusions Upon Solitude and Seclusion: A Report From New Zealand” (2015) 27 SAclJ 731.

Thomas Levy McKenzie “The New Intrusion Tort: The News Media Exposed?” (2014) 45 VUWLR 79.

Ursula Cheer “The Future of Privacy: Recent Legal Developments in New Zealand” (2007) 13 Canterbury L Rev 169.

Wendell B. Alcorn Jr “Reviews” (1968) 6 Hous L Rev 200.

William L Prosser “Privacy” (1960) 48 Cal L Rev 383.

E Restatements of the Law

American Law Institute *Restatement of Torts* (2nd ed, St Paul, Minnesota, 1977).

F Reports

Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy, Stage 3* (NZLC IP14, 2009).

G Dissertations

William Fussey “Applying and Developing the Intrusion into Seclusion Tort in New Zealand” (LLB (Masters) Thesis, Victoria University of Wellington, 2015).

H Internet Materials

Ann Cavoukian “Privacy and Drones: Unmanned Aerial Vehicles” (August 2012) Information and Privacy Commissioner of Ontario, Canada, Privacy by Design <www.ipc.on.ca>.

Hadyn Green “Drones” (21 April 2016) Consumer NZ <www.consumer.org.nz>.

Electronic Privacy Information Center “Domestic Unmanned Aerial Vehicles (UAVs) and Drones” (2016) <www.epic.org>.

Frost Brown Todd “First Lawsuit to Clarify the Rights of Drone Operators and Property Owners Filed in Federal Court” (January 5, 2016) <www.frostbrowntodd.com>.

Michael S. Schmidt and Michael D. Shear “A Drone, Too Small For Radar to Detect, Rattles the White House” (26 January 2015) New York Times <www.nytimes.com>.

Natasha Johnson “Topless neighbour’s drone picture prompts calls for privacy law overhaul” (17 November 2014) ABCNews <www.abc.net.au>.

Nick Heath “The long-range drone that can keep up with a car and fly for an hour” (27 May 2015) TechRepublic <www.techrepublic.com>.

I Other Resources

Privacy Commissioner *Case No 267458* [2015] NZ PrivCmr 6.