DRONE CAMERAS: CONCEPTUAL CHALLENGES FOR THE COMMON LAW PROTECTION OF PRIVACY

Presentation delivered to Australasian Supreme and Federal Court Judges' Conference
Canberra, 22 January 2020

Prof Nicole Moreham, Victoria University of Wellington

INTRODUCTION

- When people find out that I specialise in the common law protection of privacy they often say that things must have changed a lot with the rapid advancement of technology in recent decades.
    - My response is usually to agree although, depending on the interlocutor, I might go on to say that in many respects technology – like the drones we are discussing today – has just made us better and faster doing the kinds of intrusive things which people have been doing to each other for decades;
        - And as a result our fundamental understanding of things I write about – what privacy is, why it is important, how we should define it legally – has remained remarkably stable.
        - And the upshot of this is that, although in many jurisdictions privacy protection is only just beginning to have its time in the sun, the principles which *are* present in the common law still tend to apply pretty well to modern technological developments.
- So why then do I want to talk about drone cameras?
    - It is because all that said, the advent of new ways of interfering with people's privacy can be a useful prompt to check the appropriateness of our ideas about privacy and how we protect it.
    - So this talk is going to be about the way in which the capabilities of modern drone cameras can both challenge and help illuminate our conceptual understandings of the privacy interest and of how the common law of privacy should develop more broadly.
- The starting point for this discussion should be the technology and in particular I want to identify what it is about drone camera technology that I think is particularly significant from a privacy perspective.
- The answer to that question is fairly simple. That is that there aren't very many places that drones can't go.

- This means that there are now way fewer places where people can evade the potential attention of a camera.
    - Put the other way around, drone cameras mean that there are way more places which could be classed as publicly accessible.
- The main reason for this significant jump forward is that drone cameras disrupt traditional sightlines.
    - They can fly up high and see over walls;
    - They can look into 10th storey windows;
    - They can fly over precipitous edges and record back – in a way that even the most powerful fixed camera cannot;
    - And they can do all of this while the user remains unseen and unidentified.
    - This is the latest – perhaps the ultimate – step in the massive proliferation of camera surveillance in the last few decades.

OVERVIEW OF THE PRIVACY TORTS

- Before I talk about how privacy law does and should respond to this that, I want to give a quick reminder of the key features of the privacy actions in the various jurisdictions I will be discussing today.
    - In New Zealand we have the tort of giving publicity to private facts and the tort of intrusion into seclusion.
        - Although the question is still not entirely settled liability in both torts is usually understood to turn on two key questions:
            - whether there is a reasonable expectation of privacy in respect of the disclosure or activity in question and
            - whether the disclosure or intrusion would be highly offensive to an ordinary reasonable person.[1]
    - Despite its different beginnings, the English privacy tort has ended up in a very similar place.
        - When the Human Rights Act came into force in 1999 English courts said that the Article 8 right to respect for private life provided the final impetus to develop breach of confidence into an action which could protect privacy interests.
        - Courts threw off the remaining constraints of the breach of confidence action and developed what is now called the misuse of private information tort.

[1] See *Hosking v Runting* [2005] 1 NZLR 1.

- It requires the claimant to show that he or she had a reasonable expectation of privacy in respect of the material in question.
- There is no need to show that the publicity was highly offensive.
- As with the New Zealand tort, the defendant will have a defence if it can show that the publication was in the public interest.

- I'm not going to presume to lecture this audience on the Australian law but it is probably worth setting out that my understanding is that the common law protection of privacy in Australia is it something of a crossroads:

    - some decisions extending breach of confidence to provide protection,
    - others purporting to recognise a privacy tort,
    - and the Australian Law Reform Commission recommending that a tort be introduced by the legislature which can be infringed either by publishing private information about a person or intruding upon him or her physically.

- As for the tests which are applied in Australian law, my understanding is that:

    - some cases have applied the reasonable expectation of privacy test and the ALRC say that that test should be the basis for liability under the torts it recommends in its privacy report;
    - some cases apply modern breach of confidence requirements;
    - others still say that the question of whether the disclosure was highly offensive to a reasonable person should be the test for what is private.

- So there are quite a few different causes of action and different tests floating around our respective jurisdictions.

    - What I'm going to say today will be pitched at a reasonably conceptual level – and is therefore, I hope, of some relevance to all of them.

I. WHETHER SOMETHING IS PRIVATE IS A NORMATIVE QUESTION

- So let's come back to drones and what they tell us about the nature of the privacy interest.

- The first point that the increasing use of drone camera technology drives home to us is that whether an activity or a piece of information is private is a normative question and not a purely factual one.

    - When someone comes to court to make a claim that a particular activity or piece of information is private they are saying that this activity or this information is something which *should* be treated as private; they *should* be *entitled* to keep the information or activity to themselves.

- I'm hoping that this point is an obvious one.

- The leading English privacy decisions certainly use this kind of normative language.
    - They use the language of what *should* happen; of what privacy a claimant is *entitled* to expect.

- For example, in *Campbell v MGN Ltd* [2004] UKHL 22 at [24], Lord Nicholls made it clear that he was concerned about whether the claimant had "a reasonable expectation of privacy that [her drug taking] *should* remain private".

- But despite the fact it seems obvious, courts have sometimes taken a different approach and treated the question of whether something is private – not as a question of what *should* and the circumstances – but as a purely factual enquiry into what is actually likely to happen in those circumstances.

  Schulman v Group W Productions Ltd 955 P.2d 469 (Cal. 1998), 490

  - Supreme Court of California held that the claimant did not suffer an actionable intrusion into her privacy when a television crew filmed her being attended by paramedics at the scene of a road accident in which she was very seriously injured because "for journalists to attend and record the scenes of accidents and rescues is in no way unusual or unexpected".

  - In contrast, the claimant could have an objectively reasonable expectation of privacy inside a rescue helicopter because the court was "aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent".

  - In other words, because the media had developed a consistent practice of riding along with ambulances and publishing detailed footage of people's treatment, there could be no reasonable expectation of privacy in respect of the kind of trauma treatment they like to film.

    - But since the media had not developed that practice in respect of ambulance and hospital rooms, they could have a reasonable expectation of privacy in respect of which what went on there.

- Hints of this reasoning in England and Wales cases as well.

  - In SC case of *Kinloch v Her Majesty's Advocate (Scotland)* [2012] UKSC 62 at [19] Lord Hope observed that a person has to "expect to be the subject of monitoring on closed circuit television in public areas where he may go, as it is a familiar feature in places that the public frequent".

    - So CCTV is so common in modern British public spaces that one can't have a reasonable expectation of privacy in respect of the kind of things that CCTV cameras usually record.

- [In fairness, Lord Hope's reference to the ubiquity of CCTV cameras was probably actually an oblique way of saying that there is societal acceptance that CCTV surveillance is okay.
    - But that is not what the judgment – nor *Schulman* – actually says.]
- Bringing this back to drones, the problem with a factual enquiry into what currently happens is that it is a race to the bottom.
    - Each new technological advancement or decline journalistic standards reduces the areas of life in which one can expect one's privacy to be protected.
        - The scope of the privacy interest is set by privacy interferes themselves.
            - If journalists like to send up drones to film into prisons or celebrities' bathrooms then – on a "what is" approach – those places are no longer private. No expectation of privacy there.
        - Given that the premise for this discussion is that there are very few places that drone cameras can't follow people to, the advent of drone technology makes this kind of reasoning particularly problematic.
- The solution to this is simple – the courts need to make clear that the question whether there is a reasonable expectation of privacy in respect of an activity or of what is private more generally is a normative enquiry into what should happen/what the claimant should be entitled to expect in the circumstances in question.
    - Winkelmann CJ has been kind enough to agree with me in writing on this point and as a result New Zealand courts have expressly recognised the normative nature of the reasonable expectation of privacy test in a series of recent decisions.[2]
    - This, I think, makes us better placed to deal with the arrival of new technologies like the ones we are discussing today.

II. HOW DO WE WORK OUT WHAT IS PRIVATE?

- Moving to the second point, if it's not a factual enquiry how do we work out – normatively speaking – whether information or an activity should be regarded as private?
    - If the drone camera does come buzzing up to the celebrity's bathroom window, what tools do we use to determine whether the user is breaching the privacy of the occupant?

[2] See *Driver v Radio New Zealand Ltd and others* [2019] NZHC 3275 at [94] and *Henderson v Walker* [2019] NZHC 2184 at [202].

- I would suggest that whether something is private is and should be determined by two interlocking questions – I am going to explain the factors and then come back to their application to drone technology.

    - The first question examines *societal attitudes* to the activity or information in question.

        - Is the activity or information something which most people would think you are entitled to keep to yourself?
        - This question is very context specific but such activities would include sexual activity, things to do with the naked body, health information, the intimate workings of the mind.

    - The second question – which establishes an alternative way of showing something is private – looks at way in which the claimant him or herself has behaved in respect of that activity or information.

        - Did she store the photos on a private device?
        - Did she put a physical barrier in front of the camera?
        - Did the activities take place behind closed doors?
        - Or conversely did the claimant post a photograph of the activity publicly on Facebook?

            - This part of the enquiry, I have argued, is about the *signals* that the claimant gave that the information or activity is not for the observation of others.

    - I have developed this two-part idea in an article – "Unpacking the Reasonable Expectation of Privacy Test" (2018) LQR 651:

        - In it I argue that close analysis reveals that these two principles in fact underpin the application of the reasonable expectation of privacy test in the many dozens of English misuse of private information decisions decided since the action's inception.

        - I think it is relevant to point out that this two-part thinking also maps quite well onto the requirements of the modern breach of confidence action; this includes the way it has been applied in the privacy context in recent Australian decisions.

            - It is not uncommon for breach of confidence decisions considering the protection of personal information to begin by considering societal attitudes to the information or images in question (often under the heading "nature of the information").

            - They will usually then go on to consider the circumstances in which the information was imparted or obtained – for example was it stolen from the claimant's laptop or communicated in the course of an intimate relationship?

        - To my mind these requirements map pretty closely onto the two-part approach I'm developing.

- This highlights two things about the role of the breach of confidence action in the privacy context.

    - First, in my view it is actually a really useful tool for protecting private information and, if applied expansively, can fulfil much of the role of the tort of giving publicity to private information.

        - [*Not delivered:* Lord Justice Sedley was right then when he said in the ground-breaking English case of *Douglas v Hello! Ltd* [2001] QB 967 that even without the intervention of the Human Rights Act breach of confidence had "reached a point at which it can be said with confidence that the law recognises and will appropriately protect the right of personal privacy".

            - Although I should acknowledge that my understanding is that English courts are far less concerned about the implications of making common law remedies available in an equitable action than their Australian counterparts.]

    - Even a jurisdiction where privacy tort is recognised, there is a lot of wisdom to be gained from breach of confidence decisions about when information should and should not be protected.

        - Breach of confidence decisions are particularly useful for reminding us of the significance which people's own behaviour can have on their rights in respect of information or activity in question.

Location

- So let's get back to the relevance of all this to drones.

- The main point I want to make here is that this two-part approach – particularly recognition of the signals principle – helps us to understand the importance of the claimant's location in assessing whether something recorded by a drone cameras is private.

- There was a time when it was argued that if something could be seen from a public place then it could not be regarded as private.

    - Perhaps most significantly, the *US Restatement of the Law of Torts* (Second) (1976), para 652D says in respect of the publicity tort that:

      "There is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."

        - In other words, if you can see it from a public space, the activity is not private.

- That statement was qualified even at the time that it was written and it is clearly too simplistic an approach now.

- In my view, it is much better to see location through the lens of the signals principle. In other words, it is one of the ways in which the claimants can signal whether they regard observation is acceptable.

    - So, for example, if I go into my house and shut the door or into a changing room and pull the curtain, then as well as creating a physical barrier which prevents you from seeing what I'm doing there, I am also sending you a strong behavioural signal that your observation is unwelcome.

        - And in those two examples, this is a signal which society would usually demand that you respect.

- Once you recognise this, then it becomes clear that that *act of retreat* – going into the house or drawing the curtain – should be respected even if modern technology means that the physical barrier the person is relying in fact on can be penetrated with the use of technological devices.

    - So if I go into my house and shut the door then even though you can still fly up a drone to look through my bedroom window, that should not stop me from having a reasonable expectation of privacy there.

        - That is because by going into the house and shutting the door I gave you a clear signal that your observation was not welcome and social mores demand that – in the absence of a countervailing public interest – a signal of that nature should be respected.

- The way in which courts talk about private property reflects this.

    - For example, Thomas J. explains in the New Zealand Supreme Court case of *Brooker v Police* [2007] NZSC 30; [2007] 3 NZLR 91 at [257]:

      "The home is a place where the well-being of the occupants can be nurtured and protected and the peace and quiet provided within the four outer walls (or fences) enjoyed without unwanted intrusions. It provides its *occupants with a sanctuary, a place to retreat or repair to in order to escape from the tensions and tribulations of the daily world*."

    - [*Not delivered:* English law contain similar observations about the "sanctity" of the home in *McKennitt v Ash* [2006] EWCA Civ 1714 at [21]–[22] and about the fact that home was "a word hitherto sacred among us" (the language of early privacy case *Prince Albert v Strange* (1848) 2 De G.& Sm. 652 at 698; 64 E.R. 293 at 313).]

- What all this means is that location is relevant because of what it potentially tells us about the claimant's attitude to the information or activity in question – in other words it is a signal which he or she is given to the world.

Public places

- So far, I have been talking about *private* space but once we see location as being about signals and also becomes clear that there are some activities which might remain private even though they occur in a public place.
    - This is particularly likely to be the case the person has sought out a place of retreat.
        - Perhaps he has tramped into a remote forest park or mountain range.
        - Perhaps he has ducked behind the bushes in some remote place to go to the toilet.
        - Or perhaps he or she is a homeless person seeking out the relative privacy of an alcove under a bridge or some other urban space.
    - All of these people are signalling that outside access is unwelcome – despite the public location.
        - The signals principle suggests that in many of these situations that indication should be respected.
    - That should be the case *a fortiori* if the activity is something that most people would recognise as private under the first enquiry into social attitudes – if a claimant is toileting, for example.
        - In those situations the activity should be even more likely to be regarded as private even though it took place in public.

Voluntariness

- The second point is that the signals principle highlights in the context of location the importance of voluntariness.
    - If being in public is regarded as a signal that one accepts the potential observation of others, then it seems that the inference should be overridden if it is clear that a person has experienced something intimate or traumatic in a public place against his or her wishes.
        - It is difficult to argue that it is okay to broadcast footage of a person who has been hit by car or suffered a cardiac arrest in public because he accepted incidental observation when he went out in public that morning.
        - The signals principle tells us why that is.

III. IS PRIVACY JUST ABOUT PUBLICATION?

- Finally, drone cameras also raise questions about how far common law privacy protection should extend.
    - Should the scope of any privacy action be limited to protection against the *publication* of private information or should it extend to purely physical incursions on privacy as well?
    - Drones bring this issue home because the principal objection to the use of drone cameras is often not to the fact that the footage is likely to be disseminated but simply to observation by the drone user him or herself.
- This reminds us about an important, but sometimes neglected, part of the privacy interest: what I call physical privacy interests – about being looked at, listened to or recorded against one's wishes.[3]
    - [*Not delivered:* Although they are sometimes neglected the effects of this kind of intrusion can be significant.
        - A colleague and I interviewed the claimant in the leading New Zealand intrusion case *C v Holland* [2012] NZHC 2155; [2012] 3 NZLR 672 who brought the action for intrusion into seclusion after discovering that her flatmate had videoed her in the shower through a hole in the ceiling in the bathroom.
        - She told us that her distress and anxiety following the discovery of the videotape was so acute that she was able unable to go out in public for a week.
            - She also reported other effects such as insomnia, nightmares, mistrust of others, fear of the defendant and feelings of shame all of which continued for months after the discovery of the filming.
            - There was no publication of this material.
        - Serious effects were also reported in the evidence given in the leading phone hacking case of *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch).
            - Nearly all of eight plaintiffs in that case used visceral language like "violated" or "sickened" to describe the effects of systematic tabloid hacking of the telephone messages for a number of years.

[3] See N A Moreham "Beyond Information: Physical Privacy in English Law" (2014) 73 Cambridge Law Journal 350-377); "Liability for Listening: Why Phone Hacking is an Actionable Breach of Privacy" (2015) 8 Journal of Media Law: Special Issue on Privacy Law 155; and "A Conceptual Framework for the New Zealand Tort of Intrusion" (2016) 47(2) Victoria University of Wellington Law Review Special Issue: Papers from the 2016 New Zealand Private Law Roundtable 265.

        - Some also reported ongoing mental health problems and problems of trust.][4]

- In my view new surveillance technologies highlight the importance of protection against unwanted watching and listening in the absence of publication particularly important.

- New Zealand's tort of intruding into seclusion does this.

    - The use of drone camera technology to obtain access to people engaging in intimate activities (like say changing, sexual activity, toileting) will fairly clearly breach the reasonable expectation of privacy in an offensive way as required by *C v Holland*.

    - [*Not delivered:* Difficulty in that jurisdiction, in my view, is not to ensure that the action stands far enough but to ensure that it does not extend to far.[5]

        - The requirements of this action are currently described rather broadly and so I think there is a risk that it could encroach unnecessarily on the law of trespass and possibly also on the publicity tort if it is not carefully circumscribed.

        - My own view then is that the intrusion tort should be limited to instances of watching, listening to and/or recording people engaged in the kind of intimate acts described above – sexual activity, toileting, disrobing.[6]]

- Australian law faces a different challenge.

    - This is the one area where breach of confidence struggles to fill the gap left by the absence of a privacy tort.

    - This is because the misuse at the heart of the breach of confidence action is traditionally been *imparting information* to another person when you knew or should have known that it was confidential.

        - It might be possible to extend this to situations where no information is passed on at all (English authority to this effect)[7] but it is challenging.

        - Might be a need for more targeted intervention.

            - [*Not delivered:* Criminal law measures might be enough here. But particularly if we are concerned about compensating the claimant for any harm caused, this does seem to create an argument for a privacy tort in Australia along the two lines –

[4] See further, N A Moreham "Liability for Listening" n 3.
[5] See further, N A Moreham "A Conceptual Framework for the New Zealand Tort of Intrusion" n 3.
[6] See further, *ibid*.
[7] See *Tchenguiz v Imerman* [2010] EWCA Civ 908.

publicity and intrusion – suggested by the Australian Law Reform Commission.]