COMMONWEALTH OF AUSTRALIA

Proof Committee Hansard

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON SOCIAL POLICY AND LEGAL AFFAIRS

Roundtable on drones and privacy

(Public)

FRIDAY, 28 FEBRUARY 2014

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

[PROOF COPY]

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

To search the parliamentary database, go to:

http://parlinfo.aph.gov.au

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON SOCIAL POLICY AND LEGAL AFFAIRS

Friday, 28 February 2014

Members in attendance: Mr Christensen, Ms Claydon, Mr Dreyfus, Mrs Markus, Mr Porter, Dr Stone.

Terms of Reference for the Inquiry:

To inquire into and report on:

A matter arising from the 2012-13 annual report of the Office of the Australian Information Commissioner, namely the regulation of unmanned aerial vehicles.

WITNESSES

ALLMAN, Ms Cheryl, Acting Executive Manager, Airspace and Aerodrome Regulation Division, Civil Aviation Safety Authority

FARQUHARSON, Mr Terry, Deputy Director of Aviation Safety, Civil Aviation Safety Authority

HOY, Mr Anthony Francis, Director, VidiAir Pty Ltd.

LAKE, Mr Sean, Acting Manager, National Operations Centre, Airservices Australia

MASON, Mr Brad, Secretary, Australian Certified UAV Operators Association

MAZOWITA, Mr Grant, Manager, Standards Development and Quality Assurance, Civil Aviation Safety Authority

McCORMICK, Mr John, Director of Aviation Safety, Civil Aviation Safety Authority

Committee met at 09:17

CHAIR (Mr Christensen): I declare open this roundtable of the House of Representatives Standing Committee on Social Policy and Legal Affairs. I acknowledge the traditional custodians of this land and pay our respects to elders past, present and future. The committee also acknowledges the present Aboriginal and Torres Strait Islander people who now reside in this area and thanks them for continuing their stewardship of this land. We will start with a prayer. Almighty God, we humbly beseech Thee to vouch safe Thy blessing upon this committee of the parliament. Direct and prosper our deliberations to the advancement of Thy glory, and the true welfare of the people of Australia.

I want you all to note that these meetings are formal proceedings of the parliament. Everything said should be factual and honest, and it can be considered a serious matter to attempt to mislead the committee. This roundtable is open to the public and is being broadcast live, and a transcript of what has been said will be on the committee's website.

I welcome all the witnesses here today. Our first session is going to focus on the regulation of drones and drone technology in Australia. To give our discussion some context, and to provide us with a starting point, I ask Mr John McCormick of the Civil Aviation Safety Authority to make some brief opening remarks.

Mr McCormick: Thank you, Chair. I think it is a very good idea to have this on at this stage. I think the executive and the administration are often accused of being a little bit behind these things, but I think that at this stage we still have time to address these important issues. From CASA's point of view, our role is in the regulation of the operations, but we do not at this stage have any head of power or any involvement in privacy issues. Mr Farquharson has previously given an introduction on where we are with our UAV regulation development. So, with your indulgence, I ask him to give you a short update of where we are to put everyone on the same page.

Mr Farquharson: When we met earlier I provided the committee with a short introductory brief. I believe you have copies of it. It is important to understand that we are talking about an unmanned aircraft that falls under the genre of unmanned aircraft systems and that, within that, these are remotely piloted aeroplanes. We regulate under part 101 of the Civil Aviation Safety Regulations, which were first written in 2002 and are currently under consideration for amendment. That will be accompanied with a series of advisory circulars giving the industry guidance as to how they can comply with the regulations and policies.

Airspace provides us with an ongoing challenge, and we are certainly not in any different in Australia from other regulators around the world. The US, for example, has hived off particular areas of airspace in which these operations take place. We issue particular approvals as we can to facilitate these operations, but the operations in controlled airspace still remain a challenge for every regulator around the world.

The industry is booming. Since we last met we have issued more approvals and we have 79 in play at present with another 20 seeking assessment. We expect that this will grow very quickly over the coming year. The majority of these are in the small UAS category, but we have recently seen announcements that governments are looking at larger systems than the types we have seen. I have given you some information about that in the attachments.

The ICAO developments are such that they are considering how these devices will operate under the convention, but we need to be aware that the ICAO remit is for international operations, so the sense at present is that they will be looking at systems that are 20 to 25 kilos and above, as they will have international range. They have done a considerable amount of work to date, but ICAO does not move quickly. We will have to deal at a local level with the smaller RPAs, and that will occupy us quite considerably over the next period ahead. As I

said, all regulators around the world are dealing with similar problems. It is the explosion of small technology—microtechnology—that has allowed small devices to proliferate. They are easily acquired over the internet. In fact, you can go down to your local store and for something in the order of $650 buy a quad machine, and if you want to go into your iPad store you can buy something for a bit less. These are model aeroplanes but they do have the potential to cause harm, and that is something that we are grappling with.

CHAIR: When you say harm, what you mean specifically?

Mr Farquharson: Operate it inappropriately, not maintaining the right separation from people or flying over built-up areas. We have model aircraft rules that specify minimum heights, separation from people and separation from populous areas.

Mrs MARKUS: Could you describe those rules?

Mr Farquharson: Not above 400 feet AGL; not within 30 metres of people who are not directly involved in the activity; not within three kilometres of an aerodrome; and—

Mr Mazowita: Day visual line of sight.

CHAIR: There is no distinguishment, obviously with those rules, between pertaining to drones and pertaining to just any model aircraft?

Mr Farquharson: Those rules read over into day visual line of sight operations with the smaller commercial operations.

Dr STONE: Are your concerns around safety—perhaps interfering with some other aircraft or banging into people, or whatever—or what about privacy issues? Do you have any concerns at this stage? Is that in your remit at all to look at the privacy issues?

Mr Farquharson: We have absolutely no remit for privacy; it is safety and safety alone.

CHAIR: So safety of other aircraft or safety of civilians?

Mr Farquharson: Other aircraft; other property; other people.

Mr McCormick: Manned aircraft are built to a standard worldwide. The normal acceptable standard for large aircraft is under what is called the code of the FARs, the Federal Aviation Regulations, part 25, and the equivalent parts in the European EASA system. And that specifies the ability and the tolerances required for the aircraft to maintain heading by itself, or stability, in other words; its ability to maintain altitude; what component failure rates they have, in other words, in most of the 737-type aircraft the components are certified that they will have one failure in a million, 10 to the minus six. The difficulty with the proliferation of these UASs—and I will talk about the big ones in a second—is that they are not built to any standard. There is no international standard at this stage. So their ability to maintain altitude, their ability to maintain heading, their ability to suffer equipment failure and then not crash, have not been established. With the larger ones, which we have often seen in Afghanistan and in other places, and the global Hawk, the very large one which I think is one of the vehicles Australia is considering, they are of course built to a military specification. But there is no immediate write-over of that military specification to the civilian specification.

For some of the larger vehicles in the US, the US Federal Aviation Administration, the CASA equivalent, has issued a type of certificate for them, but it is not that its feet are made of clay; it is just that there is no international standard at the moment. Integration into controlled airspace becomes a problem both for our services and for us from the point of view of knowing just how that vehicle will react and how it will behave. So there is a risk of interference with other vehicles, interference with other aircraft, and the possibility of crashing in public areas, with the obvious response. The smaller you go, if you get down to very low weights like under two kilograms, we are really talking kinetic energy now. A two-kilogram vehicle is most probably—and we have not settled on this yet—seen worldwide as being not particularly harmful. Nothing will ever have no harm, but it most probably is as low as reasonably acceptable, or at least reasonably possible. Once you get above that, of course, the kinetic energy effects come into play. So there is much work to be done on that sort of operation around what standards the vehicle is built to. And, as you saw yourself, and as Mr Farquharson has just said, it is quite easy to order one of these things from the number one quadcopter factory—shall we say—somewhere to the north of us.

Of course, we have no ability either to interfere in what is rightly Customs and Border Protection's territory as well as in the regulation of the import of these things. So I think it is a multifaceted issue. There will be us, as far as the regulations go, so that we allow commercial operations and, of course, police force operations and that sort of thing. Then there is the vehicle itself and the regulations around that; the air services issues of integrating them into the controlled airspace; there will be the factors that you are looking at here as well; and then it will be what

Australia's position is when it comes to how people import these things, and whether there should be any other restrictions on that. Of course, I pass no comment on that.

CHAIR: I am picking up, though, that there is perhaps some concern about the growing usage of them. But really, I suppose, the question I have is, 'How different is it to model airplanes or model helicopters?' which have been in wide circulation for ages—for years, since I was a kid or longer.

Mr McCormick: With model aircraft, most people can build one almost from scratch. These are very sophisticated pieces of equipment. I dare say that what you saw today is a very sophisticated device, even though it may look relatively simple. A few years ago the technology to build that would not have been available at the affordability level where someone could purchase it. It was restricted mainly to the military world or government high-end.

There is no doubt whatsoever that if a large UAV crashes, it will not be without harm. That is one of the issues which we always have in the back of our minds. From CASA's point of view, it is anything that ACUO comes out with in their annex—and I think it is annex 11, Grant, from memory—that deals with UAVs. Even though we are a signatory of the Chicago convention from 1944, as you are well aware there is not automatic incorporation in Australia of treaty-level documents. It is incorporated as far as we are concerned via the Civil Aviation Act, and the Civil Aviation Act says at section 3A that our prime purpose is that maximum emphasis has to be on aviation safety—protecting the public.

CHAIR: Okay. Are there any further comments from CASA regarding—

Mr McCormick: Having said that we have nothing to do with privacy, if I could just leave one thought at this stage? We have a lot of operators who come to us and wish to do things with a UAS, and in fact we have allowed a particular company to use one of these vehicles beyond visual line of sight to monitor a bushfire recently up in the Singleton area of New South Wales. But quite often we have people come to use who wish to do the same sorts of things that they envisage police forces or fire brigades will do.

Our current theory and thinking is that it is all around risk, and anything that we do has to be based on consequence likelihood. When we view it in that way, the average person or commercial operator has a certain understanding of risk. I am not saying they do not understand risk, but they understand it in whatever context they have come from, whereas I do not have to explain risk to a police force or a fire brigade. Every time the police kick down somebody's door, or firemen run into a building, they understand risk. So there is less likelihood, from our point of view, that they will not understand the concepts that we are talking about when it comes to risk. Risk is a very nefarious thing; if nothing happens, there was no risk—well, that is not necessarily so. However, there tends to be that mindset.

So we are taking a graduated approach to it. What we will do with law enforcement agencies et cetera I dare say would be slightly more than we are prepared to do at this stage with a commercial operator until the commercial operator establishes its bonafides.

CHAIR: Okay.

Mr McCormick: Lastly, Chair, I see we are not on here for the rest of the day, but if you require us we are only about 10 minutes down the road. We are quite happy to come back.

CHAIR: Great—I think there will be a few questions from the committee members.

Ms CLAYDON: I just want to follow up on what you mentioned earlier. You said that you had the 79 approvals at the moment and another 29, I think, waiting. Of those approvals, can you break down whether they are primarily commercial operations or—

Mr McCormick: They are all commercial

Ms CLAYDON: Okay. Thanks.

Mr PORTER: Given that weight and size are obviously the major indicators for potential danger for this equipment, just in your recent experience what is the most dangerous piece of equipment that you have come across—in terms of kinetic energy, weight and size?

Mr McCormick: Outside of the military operations in Woomera, I do not think we have seen any large UAVs. I think the industry may be better able to tell you this. I do not think we have seen anything above a couple of kilos.

Mr DREYFUS: I would be interested to follow up on Christian's question. What is the largest UAV in operation commercially in Australia? Perhaps that is a matter for you.

Mr Mason: The largest one in our association would be 15 kilos, I believe.

Mr DREYFUS: ScanEagle is probably the largest of the Boeings that you operate here.

Mr Mason: It has been used for non-military use in Australia.

Mr DREYFUS: That is a 15 kilogram device. What is its wingspan? Is it right to talk of wingspan?

Mr Farquharson: Yes.

CHAIR: We have 3.11 metres.

Mr McCormick: Again, with those operations of the scanning ball, up until now they have some mammal survival. They are involved with the rescue operation which may come into being for the surf lifesaver associations in Australia and in Queensland. They also were the operators that we permitted to operate beyond visual line of sight outside of Singleton, in what was segregated airspace. In other words, we permitted no other aircraft in that airspace.

Mr DREYFUS: What were they doing?

Mr McCormick: I think they were demonstrating to the Rural Fire Service their ability to use a sensor system to track fire fronts. That is a worthwhile task, I might add, so it is up to us to facilitate that as best we can.

CHAIR: On that topic, we might jump over to you, Mr Mason, to give an outline of what members of your organisation are doing in this space and how widespread the usage of the larger drone technology is.

Mr Mason: Thank you. The association has 23 members at the moment who are what we call OC, operator certificate, holders. They are all commercial operators. I think the largest machine that we have in our membership would weigh about 15 kilograms. Most of them come in at under 7 kilograms. The uses are quite broad. They are for everything from standard real estate aerial photography and video through to mining surveys and stockpile surveys and there are agricultural applications for multispectral imagery, crop health, moisture content and all those sorts of thing. They are for all sorts of things—pipelines, power line inspections. Our members cover quite a broad range of activities.

From our perspective, what we are seeing is that there is a lot of illegal and unauthorised use of UAVs. We understand that the regulator is doing its best to try and combat that but, unfortunately, as the director mentioned before, they are so easily available and so cheap to buy these days that anybody can buy one and anyone can go out and operate one. It is really difficult to regulate, manage and catch those people. A lot of those people are coming from a non-aviation background, too, so they do not have an aviation knowledge set. They are coming from a commercial business background, so they are not really aware of some of the things they are doing and some of the safety implications of what they are doing. What we would like to work closer with the regulator in how we can combat that, because the greatest threat, from both a safety and a privacy issue, is more so from the illegal and unauthorised operators than the certified operators. We are heavily regulated and we are quite heavily limited in what we can do and where we can go. It is not like we can just put an aircraft up in the air anywhere at any time. We have to go through very strict procedures, quite strict safety and risk management assessments, before we put an aircraft in the air.

In amongst that of course are the privacy issues. A lot of our members already adopt a privacy policy. If it is deemed that privacy may be an issue, then we will approach the people who may be affected and at least give them an opportunity to have their say, or voice their concerns or opinions before we actually put an aircraft in the air.

CHAIR: Do you have set protocols for that?

Mr Mason: We do.

CHAIR: Do any of your members, the operators who are using these devices, use them for the collection of personal data at all? Are they specifically used for mapping and infrastructure analysis and stuff like that?

Mr Mason: The privacy issue is really to do with the data that comes from the machine. The machine itself is not the problem, it is the data that is collected. Most of the data that our members collect is collected for a client. Quite often the client will stipulate that that data must be protected and secured, that it is not freely available to anybody else. Quite often we are contractually obligated to secure that information. In other areas—public areas, or areas where the public may be at risk—then we do a full job safety assessment. With that comes a privacy assessment as well.

For instance, if we are doing a suburban photographic shoot then the potential for the next-door neighbours to be affected is very real. Quite often, it is more a perception rather than an any actual privacy risk. But we take that into consideration, and we do our best to inform most people and give them an opportunity to voice their concerns before we do anything.

CHAIR: What I am specifically asking is: is there anyone operating these devices within your organisation who is utilising it specifically for the collection of personal data, like flying a drone over to check how many sheds there are in a suburb?

Mr Mason: No.

CHAIR: Nothing like that at all?

Mr Mason: No.

CHAIR: When you talk about the unauthorised devices that are out there, are they the larger devices or are they more the ones that are easily accessible over the internet?

Mr Mason: They are more the smaller, easily accessible ones, yes. The latest incident was on the Sydney Harbour Bridge, where we had someone fly one through the bridge and it landed on the railway tracks. It created a bit of a stir there for a while. But what we did not see was any follow-up from that.

Mr Farquharson: John, was there any procedure that was enacted on that one?

Mr Mason: Yes, that is in train.

Mr Farquharson: Okay, good.

Mr McCormick: From CASA's point of view, if we now try to do something to say that you cannot operate a lightweight UAV unless you tell us—leaving aside the grey area of the model aircraft—when it becomes something that is commercially viable I would be in a situation of writing of regulation that I know I cannot enforce. That is bad law. We are hamstrung here in many ways.

CHAIR: I understand. Okay.

Mr Mason: We try to work with the regulator to find solutions to that, but we accept that it is a difficult process for the regulator to deal with. There are lots of them out there.

CHAIR: I refer to the UAVs for commercial use, rather than civilian users who are just doing it for fun and where it may get out of control and land on a railway track, Anecdotally, what have you heard some of these unauthorised users are using it for in their commercial purposes? What commercial purposes?

Mr Mason: We see a lot of UAVs used for things like real estate photography. It is big, even to the extent where we had a real estate agent in Brisbane recently who was advertising free aerial photography with one of these small quadcopters. He was completely unaware of the regulations. He put a full-page advertisement in the Brisbane papers saying, 'We will fly and capture your real estate property for nothing.' That is a big issue for commercial operators, but also for the regulator. A lot of these people, as I say, are just not aware of the safety and privacy issues. From our perspective, they are the greatest risk to aviation and public safety and privacy.

Mr Porter: I just want to touch on the issue of inadvertence, because it seems to me that this is one of the problems with responsible use of this technology. If you are viewing an industrial asset using a commercially-viable drone for real estate, or whatever it might be, you are recording metadata to assess the structure and quality of the asset. In most jurisdictions there is a formulation of words in the relevant listening devices act that stipulates what is lawful from what is unlawful, and this is a very core summary of that. That form of words usually goes something like: 'it is unlawful to record a person in any circumstances where they would reasonably consider that their activities could not be viewed by the general public'.

Mr Mason: Absolutely.

Mr Porter: It seems that the inadvertence issue is that, when you are collecting the metadata on an industrial or real estate asset, you may well be taking pictures of a farmer walking on his back porch, or whatever that might be, that potentially breaches that general rule that exists in most jurisdictions. So my question is this: do you go back over your data and expunge or adapt the data that may breach that principle?

Mr Mason: We assess the situation first to see where the perceived privacy issues are. When we turn up to a property or a client's premises, we are looking for those issues and we will note them down. If necessary, we will go and knock on the doors and talk to those people and say: 'We are about to do this. Do you have an issue? Are there any concerns?' But, on top of that, the technology itself is developing quite rapidly and there are already some technologies in place—things like automasking, for instance—that allow us to section out parts of a property or areas that we are imaging or photographing and say: 'That area is out of bounds. We do not take any pictures in that area'. There is also what we call 'geofencing', an internal software within the autopilot system that stops the UAB going outside the boundaries that we set. That in itself sets up certain boundaries that we will not breach.

Mr Porter: Is there, above all of those safeguards—

Mr Mason: There is potential.

Mr Porter: Yes, and in response to that potential is there a general routine process of assessing the data to adapt or remove information that you consider might [inaudible]

Mr Mason: At the moment it is very individual. As an association, we are currently trying to put together a proper code of conduct that will capture all of that, but that is still a work in progress at this stage.

Mr Porter: A point I would put to you and seek your observations is that one difficulty with that formulation of words that I have previously given a summary of is that it is not quite keeping up with the technology, because there can be quite reasonable inadvertence. But it seems that the offence might be committed at the very point of recording. It may be that one of the legislative responses over the broader sweep is to give some kind of reasonable time period for people to remove or expunge the data after considering it.

CHAIR: Is it possible for information purposes of the committee to get a copy of your privacy guidelines and your policy?

Mr Mason: Certainly.

CHAIR: That would be very helpful.

Dr STONE: That was exactly the question I was going to ask. Those privacy guidelines would be good. Besides that, are you taking any other country's regulations, codes of conduct or privacy codes as best practice? Are you being influenced?

Mr Mason: We are.

Dr STONE: Who do you see currently as having best practice?

Mr Mason: At the moment we are looking at UVS International in Europe. They have recently invited our association onto the international ARPAS coordination council, and in that forum we will be working on best practice that has been developed both there and here.

Dr STONE: At the moment, what do you see as the biggest difference with what we are doing? You have mentioned that you feel we are very heavily regulated. They were your words in relation to the commercial users. How are the Europeans doing things differently?

Mr Mason: I do not believe they are doing things a great deal differently. My understanding is that places like the UK and France and Belgium have a very similar system of registering and assessing operators. They go through a formal training process and an assessment process, the same as here. I believe they are very similar. There are subtle differences but, generally speaking, there are fairly common traits across it.

Dr STONE: And just to clarify, when someone goes to become a registered and commercially licenced operator, they presumably describe exactly what they want to use this drone for and that is it?

Mr Mason: Yes.

Dr STONE: At the front end they register, 'We are going to use this for real estate,' or checking stock troughs or whatever the story is, and you do not require them to update that every five years or something like that? That a one-off?

Mr Mason: That might be a better question for CASA.

Mr McCormick: That might be a better for us, I think.

Mr Farquharson: Each certificate is issued with a number of things that the operator can do, and that is all they are authorised to do. If they want to expand that or remove something then we amend the certificate through a process.

Dr STONE: So they would come back when they might choose to do something?

Mr Farquharson: Yes.

CHAIR: The policing and regulation of that must be very difficult.

Mr Mason: We have an operations manual. It is the same as the manned aircraft environment in that everything that we do is laid out in it quite specifically: what we have to do, can do and should do, and the guidelines by which we do that. Any amendments that we need to make or any changes that we want to make have to be made in that manual, and we cannot make those changes without coming back through CASA and getting approval to do that.

Dr STONE: And that is specifically designed to meet that particular commercial operator's needs? It is not a standard manual—this is a real estate photographer, so that deals with that particular purpose.

Mr Mason: Correct—each manual would be individual to each business, yes.

Mr DREYFUS: This might be a question that is more for someone who has knowledge of visual technology or visual recording technology than unmanned aerial vehicle technology. Auto-masking technology: presumably there is a whole range of things that can be done to mask, including perhaps software that automatically pixelates any human image—any face—so that the finished product does not display whatever you instruct it not to display. Is that right?

Mr Mason: That is absolutely correct.

Mr McCormick: Following on from the comments made about Europe. Europe is, dare I say it, somewhat of an unwieldy beast when you bring the EU into play. Though they still have national interests they do have an overarching safety organisation called the European Aviation Safety Authority, and balancing those national interests versus the EU interests I think is something that they will continue to work on for some time.

When we talk about privacy—and I have already said I do not have a head of power in that area—a lot of people see privacy from the United States' perspective. Of course, the citizen's rights—to use that as a working term—in the US under privacy are somewhat different to the environment that we have here. So there is a slightly different conception there. I think that where whole thing goes—and where you and the committee were obviously going Chair—is to around privacy itself and data collection. The UAS is just one part of that. Inn some respects, to a news organisation a UAS is probably just a camera on a 200-foot-high pole; there is no difference as far as that goes.

So it is a subtle mix between the ability of these things to range and collect data is, a bit like, shall we say, some time ago when Google was driving around the streets. There is always that risk if you are vacuuming up data that you will come across that. But the environment in which the individual is protected in Australia under law for their privacy, and the environment in which the companies or organisations are respected to privacy, is the cornerstone of all that. If that is established and well understood in the legislation then we can build up from there. It is a little bit like we are going back down the other way in some respects, but I appreciate that the proliferation of these things means it has got away from us a little bit. It has expanded so quickly that we are playing a little bit of catch up.

I think that, as I said in the introduction, it is very prescient that you are actually considering this now before we see further issues. But I think the UAS part of it is only part of privacy, and only part of the data collection—albeit a very big part.

CHAIR: Do any of your counterpart agencies around the world actually cover privacy to any degree? Are you aware of that?

Mr McCormick: I recently spoke to my counterpart in the Federal Aviation Administration about this. They have a plan, or they are required to produce a plan by the end of next calendar year, for the integration of these vehicles into controlled airspace. They thought that would most probably not happen, due to the sequestration situation in the US government from some time ago, but they have been funded to do that work. That means that it is not only the technical issues that we talked about before—integrating with other aircraft et cetera and the ability of the vehicle to fly. Most controlled airspace in the world is controlled airspace because it is over populated areas and large masses of people. So you can see that, by default, in allowing the integration into controlled airspace you will naturally make the vehicle able to see a greater section of humanity, shall we say. To my knowledge, they do not have any other mandate from US congress to go into the privacy area but, as I say—and you are more aware of this than I am, most likely— from the legal point of view, privacy in the United States has different meanings and different responsibilities in the common law in the US compared to Australia. I guess the short answer is: no, I do not think so; however, I think eventually it will come their way anyway.

CHAIR: Mr Lake did you want to give a quick brief to the committee?

Mr Lake: Yes, just to follow up on that—and it is just a point of interest—I was reading some information about a bill on privacy of UAVs that I believe is in Washington as of last week. I do not have the details with me, I am afraid, but it is certainly something I can pass on. In terms of the Airservices point of view, yes, we are acutely aware of the rapid proliferation of UAV operations. We are working closely with CASA and our focus is very much the same as CASA—it is on safety, totally; our remit is not into privacy. The question of integrating operations into controlled airspace, as opposed to the segregation which we have been doing up until now, is probably our primary focus.

Mrs MARKUS: I was just thinking about the certification. If there were instances of a certified UAV operator not remaining within their remit or what they are permitted to do, what would be the processes or approach from CASA's point of view? Are there penalties? How would you approach it? Has that already happened? What are the instances?

Mr Farquharson: To my knowledge it has not happened. But we do have administrative powers to vary, suspend or cancel certificates and, if we have somebody kicking over the traces, so to speak, then we will take appropriate action. That may be to constrain what can be done; it may be to say do not do that again, depending on what the particular problem was. We have a range of powers that we can use to take the appropriate action for safety purposes.

CHAIR: Mr Mazowita, you may have some more information on this proposed law.

Mr Mazowita: With respect to the situation of the FAA, I have seen recent literature where the FAA essentially acknowledged that they had no direct role vis-a-vis privacy issues but, when they issue their operational approvals, from a safety perspective they make it a condition of that approval that the operator will comply with all federal and state laws regarding privacy.

CHAIR: Mr Hoy, VidiAir is interesting because you are probably on the cutting edge of where the technology is going. Could you give us a brief on how things have developed in this space with this technology and where it is going and perhaps give some commentary on some of the issues you have heard regarding regulation?

Mr Hoy: Thank you, Chair. I have been involved for four years with UAVs and I obtained operational certification in July last year. The primary concern for me and my colleagues has been systems reliability—which is difficult to regulate and is unregulated, as things stand—to the point where we have engaged out own microelectronics engineer because of our concerns. I think it is fair to say that the general consensus on the part of insurers and many other operators is that critical systems failure is significantly under-reported, particularly on the part of the unauthorised users. I realise this is something that is impossible for CASA to have a hand on, but some of them are flying and operating very sophisticated units, not just the cheap quads. It is now quite easy for them to obtain hexacopters and octocopters, and some are happy to pay $10,000-plus. Recently our concerns were such, given our own difficulties that we had encountered, that we undertook a microelectronics audit of a $12,000 machine—a premium-brand octocopter—in order to understand the background issues that were causing problems to us and others. The audit outcomes were of some considerable concern, our interest being to come to terms with them as we work towards building an industrial standard—not the military type operation or machine that John McCormick referred to but the smaller quadcopter, hexacopter and octocopter type units. That has been our principal interest and activity as we approach our research and development tasks.

Dr STONE: Mr Hoy, you referred to real concerns you had after your audit. What sort of concerns are you talking about? Just the machines failing, or them banging into people's TV antennas, or getting mixed up in—

Mr Hoy: A lot of the machines fail—

Dr STONE: What proportion of the machines fail?

Mr Hoy: because the standard of componentry in even the premium brands is of a hobbyist standard in a lot of cases. We found vital components missing, such as decoupling capacitors. We replaced batteries with lower internal resistance and significantly higher amperage. There was just inadequate fit-out. There were battery connector plugs that were inadequate for the power required for the unit. Each of these things is capable of causing a fly-away or a crash, as does happen and is happening, I can assure you. I could go on. We actually have furnished a long list of the difficulties we encountered to various industry parties, with some considerable interest. We and others are moving towards working through these microelectronics issues to try and come up with an industrial standard. Our equipment is being laboratory tested for temperature, vibration and shock so that we can understand what might happen in a crash.

Dr STONE: So you cannot just hijack the military standards and put those across to commercial standards?

Mr Hoy: I would not—

Mr McCormick: I think the answer there—sorry, Mr Hoy—is that the military is prepared to accept losses and in the operational sphere they do accept that some of these will not come back, as we have seen reported often in the newspapers. Of course, to the civilian world that is intolerable. We would like to get that risk as low as reasonably practicable.

Mr Hoy: That is true, and we have seen quite high-profile incidents, such as the crash and burn of an octocopter in the streets in New Zealand last year and units splaying into the crowd in a Brazilian soccer stadium. So it is a concern.

Dr STONE: Are these concerns similar, or is the rate of failure similar, for the hobby, non-commercial sector, which typically has smaller, cheaper flying things?

Mr Hoy: I would say it is of greater concern, and I would think most people that are buying a certain very popular brand of Chinese quad crash them. However, it is not only the hobbyist units. In our case, we were talking a $12,000 machine.

Ms CLAYDON: You mentioned earlier that you have supplied some of the data from your audit to commercial operators, and I am wondering if you can supply this committee with any data with regard to your findings in terms of incidents that have occurred in Australia.

Mr Hoy: I am happy to furnish the audit outcome. Certainly.

Ms CLAYDON: How close do you think you are towards developing these industrial standards?

Mr Hoy: We believe that we have overcome the problems that were determined in the audit to a large extent. We have made an appointment with CASA for the second week of March to demonstrate the machine that we believe is built to that industrial standard, with a view to having our own operational certification varied.

CHAIR: Ms Allman, I am not sure if it is in your area, but how are the operators assessed for certification? What do they have to go through and how long does it take?

Mr Allman: It is certainly not my area, Chair, no.

CHAIR: Who might be able to answer that one?

Mr Farquharson: There are two aspects of certification. One is the pilot, the controller, certificate. They are assessed against a knowledge standard and a competency standard. The second part of the assessment is in relation to the operating certificate. There is an operations manual and appropriate controls put in place that the organisation has the right set of resources to do what it is intending to do. At the end of that, the person can be certified individually as a controller or an organisation receives an operating certificate.

CHAIR: Does anyone on the panel wish to add anything else before we break? The member for Isaacs just asked, particularly to you, Mr Mason, in your role as someone who is in the industry and is looking after those members, if there is anything else you wanted to add about the prospect of greater privacy regulations coming in?

Mr Mason: From our perspective—the commercial operators—we believe that there are state systems in place already that start to address it. We accept that it is not perfect and it still needs a little finetuning, but there are basic systems there that we can build on. From the operators' perspective, it is in our interests to respect privacy and safety of the public. If we are seen to be breaching people's privacy and safety then obviously the perceptions are going to increase and it will make it harder for us to do our job. All I can say is that, from our perspective, it is in our interests to address those issues and we are quite happy to engage with the committee or any other body to bring that into effect.

CHAIR: Is it dated, do you think? Do you think there is a need for some greater regulation in the privacy sphere?

Mr Mason: From the commercial operators' perspective I would say no; from the unauthorised side, most definitely.

CHAIR: Mr Hoy, you would probably be able to offer a pretty good opinion, given your background and what your company is doing. Do you think there is a need for greater regulation in this area of drone technology?

Mr Hoy: As far as privacy is concerned?

CHAIR: Yes.

Mr Hoy: I made a note for our own purposes, as I thought it was an interesting suggestion by Mr Dreyfus. I think in post production there is certainly scope to pixelate human features. In our own situation, we are mainly interested in industrial applications so that trespass, nuisance, privacy is not so much an issue. We have been working in trials, for instance, around the Port Kembla Steelworks real estate. Our approach, if we were to undertake it, would be to doorknock the immediate neighbourhood. I do not see it being such an issue, apart from perhaps in news gathering, that it cannot be addressed quite simply.

CHAIR: If there were privacy regulations put in place regarding drone technology and they were under CASA's remit, would you have the ability to handle that?

Mr McCormick: I think there are a number of issues that that would address, but I will follow on from Mr Hoy's comments before I get to that question, From our point of view, we are committed to working with the commercial operators that are willing to commit resources and go through the types of things that the other gentlemen have mention. It is the reality that these things are here; we cannot turn back the tide. As has been pointed out, what we have to do, of course, is segregate who is legal operator prepared to abide by regulation and who is not. The follow on to that is that if CASA received a remit—and it is my deepest desire that we do not

receive such a remit; I will put that on record—it would then be a case of only being able to enforce what we know about, and we would in the Rumsfeld situation of known unknowns and unknown unknowns. That is not said glibly; that is actually the state of play.

I think we could do things around the certification entry-level control. But, again, we are interested in the safety of the vehicle, not necessarily the payload that the vehicle is carrying. So if we were to go into the area of certifying the payload, such that we insisted on things such as the member for Isaacs has mentioned—pixelating photographs of people's faces et cetera—that would make it a much, much more complex operation and a much more difficult issue for us. Certifying the entire vehicle and the payload package would introduce cost complexity and delay.

As I touched on earlier on—I know it is at the heart of the committee's deliberations—privacy is a much wider issue than just UAS. This just happens to be the focal point at the moment. I think privacy should rightly live where it should. If there were to be some restriction on import et cetera, then that is a matter for Customs and Border Protection and others. If we were to look at the payload, that may very well be something that the information commissioner has a view on. Again, given the size of our agency, we have to stay focused on the safety aspects of these vehicles. As I have said, we have no concern with supporting the commercial operators and the associations which are represented here today; it is the other ones we are concerned about. So even if I have a law, they are going to disregard it because they are disregarding it now.

CHAIR: I suppose that is the case for any authority. Having said that, do you think that there is a need for greater regulation, or does the fact that it is going to be extremely difficult to police probably negate any sort of need for it?

Mr McCormick: In our sphere within the Civil Aviation Act and the associated airspace act et cetera that we work under, we have sufficient tools and the sufficient legislative head of power to do what we have to do in the safety sphere, given, as I said, the precedence to section 3, which says we have to give our priority to safety—avoiding accidents and incidents. To go outside of that, I think, would be difficult, and a parallel discussion would be about, for instance, whether CASA should also control the Office of Transport Security and its functions. That is done in some jurisdictions around the world. Australia took the view that security and safety were separate, and long may that last. So, again, it is how the parliament decides to build the animal—so to speak—that will determine where it goes, but we certainly do not have the resources or budget to do the sort of operation required to do it justice on the privacy side.

CHAIR: Let us say that it did not go within your remit and that we are just talking about privacy regulations with an authority of some description that was looking after that. Do you think that it is needed, that it is self regulating at the moment and is okay or that it would just be unenforceable so it is probably useless to even talk about it?

Mr McCormick: I think the situation at the moment, and what I am hearing, is that the industry seems to be self regulating on the privacy side. There will of course be people out there who are flaunting that—the illegal operators. So the status quo may be acceptable, but the thing is the proliferation of the number of people applying for operating certificates, as Mr Farquharson said. We assessed a while ago that for every UAV we knew of there were six that it would did know of. I am not even sure whether that comparison is correct anymore. It has most probably gone even further away than that; that was over a year ago that I made that statement in Melbourne. The known unknowns! So it fits where we are today. But if you are looking to put in place a mechanism which will outlive the next couple of parliaments, for instance, hopefully with constant updating, then I think you have to do something to be honest.

CHAIR: Mr Lake, do you want to offer opinion on that from Airservices Australia about the need for privacy regulations?

Mr Lake: I do not think, to be honest, that I am qualified to common on it, Chair. From a personal viewpoint, not professionally, it seems to be the case.

Mr DREYFUS: Mr Mason, I want to thank the association for a very helpful submission. I just want to tease out a couple of things from it. First of all, you have got a voluntary code of conduct that the 70-odd members of your association have agreed to be bound by.

Mr Mason: 23.

Mr DREYFUS: Sorry, 23.

Mr Mason: We only represent about a third of the industry, at the moment.

Mr DREYFUS: Sorry, there are approximately 70 commercial operators, but you represent 23.

Mr Mason: We represent about a third of the total AC holders at the moment.

Mr DREYFUS: You do not speak for the remaining 50-odd and you do not know whether they abide by that code of conduct or conduct operations in accordance with it?

Mr Mason: The reality is that we do not know what those other operators are doing. We have no control over them. From an association's perspective, we try to act in the best interests of the industry as a whole not just for our members. We are very democratic, open and transparent about how we do that. We try to engage the rest of the industry as best we can, but obviously it is up to them at the end of the day whether or not they chose to join us and come on board with the procedures, systems and policies that the association is trying to put in place.

Mr DREYFUS: For this code of conduct, could you sketch what sources were used in putting that together—in other words, did you look at particular other countries or other particular documents that were helpful in compiling that code of conduct, which, helpfully, you are going to produce to the committee?

Mr Mason: As I say, the code of conduct is still a work in progress. We have drawn on a number of sources. You UBS International has a number of resources available to us. We are still wading through a lot of that. The Privacy Act puts in place certain procedures and policies that we have to abide by. There are legal measures that we have to abide by from a state perspective and we have employed those. It is still working progress; we have still a bit of work to do to finalise that code of conduct and get it signed off. Some of the members, as you can probably appreciate, are a bit hesitant sometimes to adopt more regulation and more policies that are going to govern them. We feel that we are already quite heavily regulated as it is. As I said earlier, it is in our interests to make sure that we operate safely. It is the social licence, if you like. If we do not abide by certain procedures then perception that we are doing the wrong thing increases quite dramatically, and that just makes our work and our business that much harder to do. We are doing our best to put policies and procedures in place, but it is still a work in process.

Mr DREYFUS: You touched on that social licence concept earlier in your remarks. I take it that your association's purpose in having this voluntary code of conduct is that it might spread so you get higher levels of compliance with it. Part of your objective is to build confidence in the community in relation to your operations so that people can have more confidence in the safety levels, the things you are operating, and perhaps also more confidence that there will not be intrusions into personal privacy from operations that your members or any commercial operator are conducting.

Mr Mason: Absolutely.

Mr McCormick: Chair, sitting behind us is Ms MacTavish, who is the Executive Director of the Australian Association for Unmanned Systems—AAUS. She most probably would have a few things to say about this from her members' point of view—on indulgence, if you allow her to join the table.

CHAIR: Very happy to.

Ms MacTavish: Would you like a brief overview of our association?

CHAIR: Please.

Ms MacTavish: Our association was established in 2009 and began operations in 2010. We work very closely with academia, government, the military and our industry representatives. We have a board of directors—15 in total. We work directly with CASA to participate on the industry boards, to make sure that we are there for the regulation, and we have been a part of setting up the advisory circulars that are coming forward. We work extremely closely with academia to look at the collaborative efforts where we can produce our technology with industry.

We have at present just over 430 members of our association across Australia. We were affiliated in the beginning with AUVSI from Washington DC, but we became our own organisation in last March—2013. We work very closely with the Department of Defence, as well as the military. We sit regularly with the Army, Air Force and Navy to make sure that we have representation there.

We host major events across the Australian association with the Avalon Airshow Pacific, and this year we will begin with land forces. We also conduct seminars and workshops across the country in all areas of the industry and domain. So we represent unmanned systems in the air, but also terrestrial and maritime as well.

CHAIR: Can you give an outline—and it is probably a lot given that your membership is quite large—about what sorts of purposes and uses of unmanned aircraft that your members find useful?

Ms MacTavish: Useful in the commercial sense? Is that where we are going?

CHAIR: Is that primarily commercial?

Mr DREYFUS: Can I ask a preliminary question to that? You have terrestrial and marine systems as well as aerial systems?

Ms MacTavish: Right. But the bulk is aerial.

Mr DREYFUS: Okay, thanks. Sorry to interrupt.

CHAIR: It is all commercial use, I gather?

Ms MacTavish: A lot of our members are also academic, so we have to keep in mind that there is R&D involved as well.

CHAIR: What are some of the major uses, specifically?

Ms MacTavish: Because we represent such a depth and breadth of industry, we have some of the largest operators—multinationals. If we want to take a look at membership, we have: Thales, Aerosonde, Insitu Pacific Boeing, BAE Systems, Lockheed Martin, Northrop-Grumman and Cobham-General Atomics. So we start from the very big and then we move down to our medium-size companies, and these are not just companies that are operators but they are also in the area of manufacturing. We have Yamaha, so of course we are working in agriculture. We are working now directly with mining companies, and so we have depth and breadth in many areas.

And, yes, we do represent a large number of small operators as well; so individuals, or entrepreneurs or very small companies that are two to 10 people. Some of these do operate in the area of, as was mentioned already, real estate or smaller operations like that. But we work very closely with the community and our network to ensure that the areas of privacy, standards and conducts are understood to being in progress—that we are setting up the infrastructure in this country. Without the infrastructure we will never have a viable industry, so we have to work very closely with CASA, with the privacy commission and with everyone to make sure that that infrastructure is in place.

Mr DREYFUS: Can I ask one other preliminary question? Do you have shared membership, or overlapping membership, with Mr Mason's organisation, or are you rivals?

Ms MacTavish: I do not see us as rivals!

Mr Mason: Getting straight to the point!

Ms MacTavish: No, we are certainly not rivals. We have met together and at times, I believe, we have had overlap of membership.

Mr Mason: We have.

Mr DREYFUS: I can see the potential: you have manufacturers and a much broader spread, but, potentially, you have operators in there as well.

Ms MacTavish: Yes, we do.

CHAIR: Do you have a code of conduct in relation to privacy, similar to that of Mr Mason's organisation?

Ms MacTavish: A code of conduct? No. What we have done is work directly with civil libertarians and the law firm King & Wood Mallesons, and we have just presented to the Attorney-General an entire re-vamp of surveillance and privacy. That is before them, and that is the work that we have done over the past 18 months.

CHAIR: Could you give us a bit of an insight into that or is that information commercial-in-confidence at the moment?

Ms MacTavish: I cannot. But what it does do, as John spoke to earlier, is take unmanned systems away from being, let's call it, the prime suspect and put it into the perspective of everything that can invade privacy, right from your phone to a camera on a stick. It puts into perspective any technology that can surveil or invade privacy.

CHAIR: I suppose, though, from the general public's point of view, while you can walk down the road in a public place and take a photo, or your neighbour might be able to put an iPhone over the fence and take a photo, you can fly these things over people's yards and over their houses and look straight down on them and get a pretty good shot. There is a little bit of a difference with that technology and its ability to invade other people's privacy.

Ms MacTavish: We have been very cognisant in terms of what a commercial use is and what the responsibility of that commercial use is. We have also been very careful to allow the public to have their ability to have recourse and to set out what those rules will be to have recourse. We have been very cognisant of both sides of the equation in setting up what we have done.

CHAIR: I asked Mr Mason about his membership and the uses that it has. Are any of your members utilising this technology specifically for the purpose of personal data collection—for instance, is local government using it to monitor who has got a fenced pool. Is there anyone in your membership doing that sort of stuff?

Ms MacTavish: Certainly not to my knowledge, it is certainly not something that we would condone. Again, it has to follow whatever their operator's certificate denotes them to be able to do. I don't believe that there is any such activity.

CHAIR: On that point, is CASA aware of any such activity by, say, local governments or even private organisations that are specifically doing personal data collection by flying over homes and neighbourhoods?

Mr McCormick: No, not to my knowledge. We will go back and see if we have got anything back at the office. But, no, nothing comes to mind.

Ms CLAYDON: Ms McTavish, given that you do not currently have this code of conduct, but are working something up and that something is currently with the Attorney-General, how are you dealing with contemporary circumstances?

Ms MacTavish: One of the things that we have done to address building the infrastructure is working directly with insurance organisations across Australia. At present, if you want to operate commercially you have to be aware of the fact that there are liability issues. We have set up a set of standards whereby our organisation will audit a company that wants to obtain insurance. We will go and check that you have an operator's certificate, that you are in good standing as a business and that you have no record of accident. Based on that we will make a recommendation for insurance to be sought. In a way that is a code of conduct. What we are doing is really certifying that a member is in good standing before we would recommend that they actually be able to operate with insurance. We can't, of course, recommend that they be operators—that is up to CASA. But we work directly with CASA, participating on the working committees to ensure that the regulations make sense. If we have a member that we do not feel, in our assessment, is operating within their operating certificates, we certainly communicate with CASA.

Ms CLAYDON: Would you be looking at any known breaches with that operator? I suppose particularly if there were known breaches of privacy, although I accept that may not be well known, would you look at a record of breaches in terms of determining who you want to endorse?

Ms MacTavish: It is not something that we have done in the past. Once we understand where the paper that we have written for the Attorney-General based on privacy and surveillance goes then we will have a better understanding where our purview may be in that area.

CHAIR: Earlier this week, coincidentally enough, *Stock & Land* had a report in it about the organisation Animal Liberation utilising drones to actually fly over farms to capture if there is any sort of cruelty to animals or any breaches going on. Are these guys registered with your organisation to do that activity?

Mr McCormick: We will have to take that on notice; we will get you the answer before the end of today. What we put out to people who are operating these vehicles is that, because we go into an area where the law seems to be silent when it comes to neighbouring properties et cetera, if you are intending to operate these over someone else's property you obtain their permission before you do so, more as a matter of good manners than any legally enforceable rule, from our point of view. We will get look at that and get back to you as soon as we can.

CHAIR: So if an organisation, whether it is Animal Liberation, or whatever, specifically turned up to CASA with an application and said, 'We are using this for the purpose of obtaining information because we think those people are doing the wrong thing,' what would be CASA's response? If they met all the safety guidelines and the operator guidelines, would they get a tick-off on that application or not?

Mr McCormick: Again, I think the mens rea of the whole thing is not necessarily within our remit. If someone comes to us, unless they are proposing to do something which is egregiously illegal or obviously is something which would appear to be something we needed other advice on, such as if someone said they are showing up and they wish to fly drones all around Holsworthy or some such thing, then it would behove us to go to someone else, another department, and see whether this was something in the best interests of the Commonwealth. Having said that, the Civil Aviation Act, which of course was written before drones and operating certificates came round, basically says if there is a set of requirements that someone has to meet to get a certificate, say to be an airline or to be a maintenance organisation, if they meet those requirements then I must issue the certificate. I do not have discretion not to issue the certificate. At this stage, we are taking that same approach, as we do through all our certificates and approvals. So if someone came to CASA and said that they were going to go out and check on animals et cetera in the scenario that you have put forward, unless there was

something that was illegal or would appear to be against the intent of our approval processes, then we may very well have to issue them a certificate.

Mr DREYFUS: Mr McCormick, that is because you are not looking at purpose. You are looking entirely at safety requirements; looking at the device perhaps for some purposes and looking at the qualifications of operators for other purposes.

Mr McCormick: Yes, I think that is very much the case. We have been talking about cameras, in other words, having some Olympian view or a god's eye view—because a lot of these smaller vehicles have what they call first person point of view; in other words, it is as though you are sitting in the vehicle—and these are the ones where we have seen in other states, I do not think so much in Australia but certainly in the United States, people hovering outside people's bedrooms et cetera, in an area where people could reasonably expect not to have to be concerned about their privacy. That is where we get into this area of the payload versus what the vehicle is like. At the moment there is a great risk from CASA's point of view that if we start to be involved in the payload it will continue to creep; we will have no end or no defined point where we will be able to say to somebody, 'In law that is legal;' 'In law that is illegal.' And that is not really our role, as you quite rightly said. Our focus is on the safety and the safety around the vehicle, and unless there is something that would tend us to seek advice from some other department, we would be more or less compelled to issue the certificate.

CHAIR: Thank you very much everyone for participating in this round table session. As a committee we are going to report back to the parliament outlining some of the issues that have been raised here today, and in the following sessions we are going to hold. We will consider how those issues should be pursued, or if they should be pursued at all, and the secretariat will make sure you are kept informed when we report back.

Proceedings suspended from 10:35 to 11:15

ALDER, Mr Richard John, General Manager, National Aerial Firefighting Centre; and Australasian Fire and Emergency Service Authorities Council

CORCORAN, Mr Mark, Private capacity

GIUFFRE, Mr Emmanuel, Legal Counsel, Voiceless, the animal protection institute

HARRISON, Commander Mark, Manager, Forensic Operations, Australian Federal Police

JAMES, Mr Chris, Assistant Director, Workforce Skills, Minerals Council of Australia.

MacTAVISH, Ms Peggy, Exeuctive Director, Australian Association of Unmanned Systems

MEJIAS ALVAREZ, Dr Luis Oscar, Senior Lecturer, Australian Research Centre for Aerospace Automation. Queensland University of Technology

ROBERTS, Mr Chris, Managing Director, Parrot ANZ Pty Ltd

ROBERTS, Dr Jonathan, Research Program Leader, Autonomous Systems, Commonwealth Scientific and Industrial Research Organisation

WHOWELL, Mr Peter, Manager, Government Relations, Australian Federal Police

CHAIR: Welcome. Please note that these are formal proceedings of the parliament. Everything said should be factual and honest. It can be considered a serious matter to attempt to mislead the committee. This roundtable is open to the public and is being broadcast live. A transcript of what is said is going to be available on the committee's website. Do you have any comment to make on the capacity in which you appear?

Mr Corcoran: I am a research student at the Graduate School of Journalism at the University of Technology Sydney—I am also an ABC journalist—where I lead a research project on news-gathering applications of the technology.

Mr Roberts: Parrot are the largest creator and manufacturer of consumer drones.

CHAIR: Thank you very much for participating here today. We are now moving into a session on the applications of drone technology. As a starting point, to provide some context about this part of our roundtable, I ask Dr Alvarez, given your expertise in this field, to kick off this session with some brief opening remarks about drone usage, the applications that we are finding in Australia for drone technology and where it is all going.

Mr Mejias Alvarez: The potential applications of unmanned aircraft in a civilian context are many and varied. The capacity of these aircraft to assist humans in performing dangerous and repetitive tasks in remote or inaccessible areas is significant and certainly worth exploring. This potential is one of the reasons for this forum today. The term 'drone' itself is an emotive term with the potential to conjure images of military applications, enhanced to promote fear.

For this reason I prefer to replace the usage of this word with the term 'unmanned aircraft'. So an aircraft with an appropriate set of on-board sensors that can be deployed swiftly and that can fly for extended periods of time can, for example, assist in the rapid assessment of natural disasters and emergencies, enabling a fast and well-informed response and hence reducing the impact of these occurrences. In an agricultural context, this aircraft could assist with tasks such as crop dusting, aerial mapping and wheat management, and in a marine context with the identification and tracking of sea animals.

These are just a few of the multitude of possible applications where unmanned aircraft could be, and are currently being, used to human advantage. In the short term there are some technical challenges that need to be addressed; however the integration of unmanned aircraft into civilian airspace is certainly feasible, given that the appropriate regulations are in place to ensure the safety of the operation. With a concerted effort from researchers, industry, regulatory bodies and from our government, the widespread adoption of this technology is viable and the potential gains from its usage are immense.

CHAIR: Thank you very much, Dr Alvarez. We will go all around the table and get some different perspectives from some of the major users of the technology. I will start there with you, Mr James. From the mining industry's point of view, how are you utilising drone technology? I will probably pose the same question to everyone—how are you utilising it, and how are you ensuring that there is not an impact on people's privacy from that use?

Mr James: Just to give it some context, it is very much seen as an emerging technology in the mining industry. It is not in widespread use at the moment, although it is being considered or tested by some companies. A couple of companies have actually used drones for a range of purposes; the uses range from stockpile

surveying, environmental scanning/monitoring; fire monitoring; subsidence monitoring; pit wall mapping; infrastructure assessments; general aerial photography; blast monitoring—because the UAVs can fly through a blast cloud; and also spare parts transportation out to LNG rigs out off the North West Shelf is something that is being considered.

The main benefit is safety. Company policy in the mining industry is generally to separate staff from hazards; so if you have a situation where you are looking at a rock wall, you do not necessarily want to send the surveyors in but you can send a drone in to have a look. The quality of the photography is such that it probably does as good a job as the surveyors in that sense. Furthermore, it limits the use of fixed-wing aircraft, which have their own hazards. Drones are probably seen as more efficacious in that they can hover, and that they can be sent to a location a lot more quickly than a light aircraft.

The other issue is cost. At the moment it is coming into a favourable point in the cost curve, particularly in terms of high-level photography. It is cheaper and quicker to fly a drone out to a remote region than to send a surveyor out. Still though, it is an emerging technology, and is something that is being looked at.

Privacy is not seen by the companies as a major issue at the moment, although this is an emerging space—firstly, because of the remoteness of those mining areas. Also there are many cameras around a mine site, so the mine site is heavily surveyed anyway. In terms of the privacy of the content taken by the drone, it would seem to be okay if that material is held by the company. The other issue with landholder consent—not so much in the mining industry, it has been more of an issue in agriculture—is the notion of activist spying using UAVs. I am starting to get some comments from members saying, 'Look, maybe there should be some controls about where these UAVs can actually go'.

CHAIR: Mr Alder, you are in another sector which utilises these unmanned aircraft. Again, the same questions: how are you using it, what are its applications and how are you dealing with the privacy issues?

Mr Alder: Like in the mining industry, it is very much an emerging technology—quite rapidly emerging in the last 12 months or so. Can I just say at the outset that our sector is certainly very interested in the possibilities offered by the technology and very keen to work with the industry and the regulatory authorities to explore those opportunities. We see there are a quite a number of opportunities that could be exploited and some that are currently being exploited. The obvious opportunity is the gathering of information—information which would in an emergency incident support the management of that incident, helping in making strategic and tactical decisions, and also obviously getting information that would support the provision of warnings and information to the community regarding those incidents.

There are a number of other potential applications one of which might be, for instance, provision of communications in black spots and so on through communications relays. We are interested in looking at the possibilities for actually firebombing, delivering suppressant or retardant from UAVs, but that is probably still a little way away, unfortunately. I think we have got the time to work through some of the implications of that. Currently, the very same type of aircraft that we use for firebombing are operating as remotely-piloted vehicles in other countries, so perhaps it is not that far away or as far away as we think. Possibilities range from the small UAV that might be operated locally—a classic application is the sort of binocular-type application where a local firefighter or incident commander just needs to see over the trees and can put up something locally to get a better view of what they are tackling—right through to the strategic surveillance opportunities and even through to the technologies that operate at much higher levels, Stratellite-type technology. We are looking at all those possibilities, but clearly the immediate focus is on the smaller technologies that have become rapidly more available in the last 12 months or so and are able to be operated in a less constrained regulatory environment than the medium and larger UAVs.

A number of organisations in our sector do already own and operate UAVs. For example, the Melbourne Metropolitan Fire Brigade has acquired a quadcopter-type UAV and it has been used to good effect just in the last few days. I think everybody would be well aware of the fire in the coal pit at Hazelwood, where it has been used successfully. We are looking at a whole range of applications—as Dr Alvarez said, the sorts of situations we are looking at are repetitive tasks, potentially dangerous tasks and dirty tasks. Having said that, we need to take a very measured approach to this. There is some, if I can say, hype around the possibilities that can be offered and we need to look very clearly at whether these sorts of capabilities are offering something that really is safer or more effective or more efficient than what we currently do—the capabilities that we currently have largely through crewed aircrafts. Certainly we see there are some possibilities, but we need to take a measured approach.

On the privacy consideration, it is important to remember that there is a big sector of the UAS or UAV industry that is not necessarily a commercial operator and therefore is not subject to the requirement to gain an air operator's certificate. It still operates potentially legally because it is not for commercial purposes and obviously

we are very much sitting in that sector. We have got a sector that has 40- or 50,000 paid employees and a quarter of a million volunteers. A lot of those volunteers are going to be very interested in this sort of technology, so we are very concerned to make sure that as things develop, those UAVs are operated safely and legally as well as effectively and efficiently. We will need to give some guidance to our organisation, some consistent guidance, to make sure they can do that. It would be fair to say privacy is a developing concern because of the nature of the areas in which we operate; it has been less of a practical issue but it is clearly something that we do need to take account of in the future.

CHAIR: We are going to skip down to, again, Ms MacTavish, because you represent a large range of users of these systems. You already detailed in the previous session some of the uses that are going on and I realise that you have got some work going on with the Attorney-General on this issue but how, currently, are you dealing with the privacy issues in your industry?

Ms MacTavish: Again, much as what Mr McCormick displayed, because we are not necessarily in control of that, what we do with our members, however, is make sure we take care and responsibility to be aware of what their activities may be and in doing so we advise them with respect to, again, duty of care, understanding the law, and being apprised of what the current law is. If we feel that perhaps there are activities that would not be in anyone's best interest, we certainly advise them again to go forward and make sure they understand what they are doing before they do. That goes right hand in hand with insurance issues, liability issues and privacy issues, and we do stress to the operators that they have duty of care and responsibility and that being a part of our association goes hand in hand with that.

CHAIR: Do you provide educational material and information on the privacy issues to your members?

Ms MacTavish: Yes. Whether we are in a reactive mode or proactive mode we take the approach of both, so when questions come to us we point our members in the right direction, we provide them with the information or we put them in touch with the relevant organisation so that they have first-hand knowledge.

CHAIR: Dr Roberts, does CSIRO operate, I was going to say the word again, but I will go with unmanned aircraft systems, in its uses?

Dr Roberts: Absolutely. We have used them since 1999, so quite a long time. We are in our 15th year of operating unmanned aircraft. Of course, we have increased use in the last few years as they have become more available and easier to use. We generally use them for our research in survey type activities, as you would expect, where we need to place cameras above experiments. We have examples where we have used them for crop monitoring, where we are doing plant breeding—we are breeding wheat crops and we fly unmanned aircraft above them there. CSIRO has used them for beach surveys—for rubbish that washes up on the beach—and for doing coastal surveys and they are very useful for getting good imagery so we can actually count rubbish on the beaches. They have been used recently for bushfire-spread experiments—during experiments of controlled burns, actually having a platform above there so we can monitor how the experiments are going. We use them generally for mobile robotics monitoring; we have a program where we are developing robots on the ground and it is very useful to see how they are operating from the air. We have also used them for testing equipment that we put on animals that we are monitoring. So we have work on monitoring flying foxes as they are flying around—we are trying to understand how flying foxes actually fly. Sensors get placed on the flying foxes but to test those sensors out we use unmanned aircraft. Our unmanned aircraft pretend to be flying foxes. We can then test the equipment before we put it on the real animals so that we can minimise the experiments on real animals—it is all about animal welfare, in that case.

As far as privacy goes, there have not been many issues so far because of the nature of our research. It tends to be in controlled areas or in more remote areas where we have control of that area. And everything is kind of looking down at our particular experiments. To this point we have not really had to address the issue in any substantial way; but we think that as our experiments get closer to populations and people we will have to start thinking about this, obviously.

CHAIR: So with the committee—painting the picture of how I think we will do the session—we might have a discussion now about what has just been said, because I think that certainly with media, police and community activism, we are going to go down a few different pathways on all three of those issues. I want to get to you, Chris, a bit later, given the issue of non-commercial uses or more recreational uses. Could we perhaps focus as a committee now on what we have just heard and any questions that might arise from that?

Mr PORTER: I will start. This is similar to an observation I have raised previously, but it seems most relevant to commercial, industrial and scientific uses—a question about inadvertence. In most jurisdictions there

is legislation which pertains to the use of optical and audiosurveillance devices. I am just familiar with the West Australian one, but I will read you the definition from that act of 'private activity', which is said to mean:

… any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed; …

And flowing from that definition will be restraints on optical or audiorecording of a private activity. There are certain exceptions to those broad constraints but my question, or the observation on which I seek comment, is that within industrial, scientific and commercial applications it seems there is a fairly high probability of inadvertent breach of that general principle—not to record optically something that would otherwise be a private activity. It might be a farmer kissing his wife on the back porch, or whatever it might be that may inadvertently be recorded.

I guess my question is: is that a concern? Has it occurred to anyone's knowledge? And is there a process for washing back over the optically recorded metadata to see whether or not there has been a breach and then to expunge or redact material that might be offending the law in this respect?

CHAIR: I think it would be more of a concern if he were kissing someone other than his wife for him! Again, I throw over to you Mr James to start off.

Mr James: I think one of the ways of dealing with that is disclosure: actually indicating to all parties that you are using unmanned aerial vehicles. The feeling among our companies is that it is not a major issue because there is a lot of CCTV on site anyway for various reasons—generally to do with safety—and that is quite rightly disclosed.

In terms of the unmanned aerial vehicles that are used in our industry, they would be at reasonably high altitude and so they would not necessarily pick up human activity as such and would not be designed to. I think the broad answer to your question would be disclosure.

CHAIR: Do you currently do that disclosure to property holders?

Mr James: I could not answer that question; I would not know.

CHAIR: Possibly different policies for different companies?

Mr James: Yes, it is very much an emerging area.

Mrs MARKUS: Chair, if I could just come to some of your comments, Mr James, are you saying that the unmanned aircraft would only be used within the confines of the mine? My question is moving in the direction of: is it used in exploration, and so would it be over properties that are privately owned?

Mr James: Well, it could be used for exploration.

Mrs MARKUS: Is that happening now?

Mr James: Not that I know of. It is generally used actually on site.

Mrs MARKUS: You made a comment that because of the high altitude the unmanned aircraft it would not be able to obtain the visual information that Mr Porter is referring to. My understanding is that the development of camera technology is such that they would be to identify quite personal details from a high altitude,

Mr James: My understanding is that that would depend on the type of drone that was being used and that it would also depend on what the drone was being used for—what the purpose of the drone was. It would not be designed to pick up human activity in the mining industry. The intention would be to look at rock walls, to look at pits, to look at stock piles—that sort of thing. It is still a bit of a regulatory black hole.

Dr STONE: I can see great opportunities for industrial intelligence collecting, commercial-in-confidence—especially with CSIRO experiments, what was the crop response like with product A versus product B and so on—I guess the whole intellectual property protection area. Has that come into thinking of CSIRO.

CHAIR: I want to make sure we fully flesh out the Mr Porter's question, but we will go to you, Dr Roberts

Dr Roberts: From an IP point of view, so far we only monitor our own research so, no, that has not really come up, it is all confined. Talking more about the privacy aspect of these things, we just heard that high altitude is often used in mining. In our applications we have actually got the reverse. Most of our experiments are actually very low level. The sensors, the cameras, are looking directly down at the experiments which means that any inadvertent filming away from the experiment is extremely unlikely, in fact it is more unlikely than if you were filming from a pole or something like that where you have to look out sideways; you would be more likely to see inadvertent things there. When you are looking right down, focused on the experiments, it is extremely unlikely you will see anything. That is how it has been contained at the moment in the research area.

Dr STONE: You can see the possibilities or the probabilities, where you are being highly competitive.

Dr Roberts: Yes, that's right. It has been very constrained at the moment and is within our own research facility. We are not doing work on other people's land, monitoring these crops. At the moment it is just for breeding, where our scientists are actually doing the experiments themselves. But yes, you are right.

CHAIR: Mr Allman, would you like to add to this?

Mr Alder: It is certainly an issue for us, bearing in mind that operation of unmanned vehicles in our sector could be through a commercial operator who is providing a service and who has gone through all the certification procedures. It could be a vehicle that is owned and operated by a service, like a metropolitan fire brigade. At the other end of the spectrum it could be a vehicle that is owned and operated by a volunteer member of a service who has brought it along with them in their response capacity, hopefully with the intention of being helpful.

It has not been such an issue to date, because of the nature of the areas in which we operate, fire grounds and so on. There has been not a high probability of an inadvertent beach, but clearly that probability is increasing as more devices become involved. I think it is something that we need to tackle. Coincidently, we had a meeting of a technical group yesterday to develop guidelines for the agencies on the operation of UASs. The issue of ensuring that the operations were legal from an airspace regulatory point of view and a privacy point of view certainly came up. I think we came to the conclusion that we needed to seek advice, because we were talking about state legislation, Commonwealth legislation, privacy legislation and surveillance devices type legislation as well as legislation that supports fire and emergency services, which can sometimes provide some authorities that other operators might not have. It is a complex area that we will certainly need to explore.

CHAIR: So for the end users of this technology, particularly from a commercial sense, it is quite difficult to navigate all of the rules and regulations that currently are in existence is what I am hearing from you—is that correct?

Mr Alder: Certainly, the technical group yesterday found that it was something we would need to seek further advice on—the potential for conflicting and overriding legislation.

Mr PORTER: Chair, my point would not be a criticism of the applications, they seem very sensible, but with respect to state and commonwealth legislation none of it seems to really deal with the issue of inadvertence. Some of it deals with disclosure and consent, which naturally enough is logical, but say for instance with the use of a whole range of technologies but increasingly, I understand, with UAVs with Google Earth, Google Earth is full of material which has been optically recorded which it seem prima facia would breach the type of provision that I read out earlier, but none of the legislation contains any kind of way to deal with inadvertence.

Mr Alder: I think that is true and it is my understanding at least with some of the state legislation, and please correct me if I am wrong, that the offence is actually committed at the time of the recording. If it was able to be dealt with a bit later in the chain of custody, that may be useful; but then again we are talking about, as I have said before, a sector that includes volunteers and so on, and ensuring that chain of custody could be difficult for us as well.

Mr PORTER: That is why I make the point about some kind of reasonable time period to redact or remove information, which does not really exist at the moment. As you point out, that in itself would not be easy because you are dealing with metadata—if you are commercially visualising a pipeline over a thousand kilometres, who knows what information is picked up and how you would expunge it.

Mr Alder: It has certainly been an issue for us. One of the most probable applications for UAVs is rapid damage assessments. So immediately after a fire or some other incident, it is a niche UASs can clearly operate in. There is a potential for inadvertent privacy breaches in that situation. There are also specific issues around enforcement and arson, but it may be best to defer to our colleagues in law enforcement on that issue, yes.

Ms CLAYDON: Obviously there are some tremendous possibilities for application in your area, and you outlined some of those, but one of the big challenges that I picked up from you was that whilst you have 40,000-50,000 paid employees, you have a quarter of a million volunteers operating in your service as well. I am just wondering how you currently manage any requests—I am not even sure how it comes to your attention—that some of these volunteers may wish to make use of what I am going to refer to as unpersoned aircraft, and then how you juggle what could be quite a tension, I would imagine, from time to time.

Mr DREYFUS: Can I just slightly add to the question—do you have rules already for use of non-service equipment by volunteers?

Mr Alder: Yes.

Mr DREYFUS: Would potentially that fit into those rules?

Mr Alder: It does—and if it helps we use the term uncrewed aircraft! The good news is that the volunteers are part of the organisation and subject to the rules and guidance of the organisation. It would be naive to suggest that even all paid employees as well as volunteers always went with the rules and that is something that we need to confront. Largely, we can issue guidance, we can put in place constraints about how those are used at a fire operation or some other emergency incident—that is certainly possible, and largely that is in place now. I think we do need to update it, and that was the purpose of the meeting yesterday, to make sure that the current rules that are in place to constrain people bringing personal or other equipment into an emergency environment properly reflect the nuances of UAVs. There are also a range of issues around the people who are not constrained by those sorts of rules—casual volunteers and organisations just wanting to help. News-gathering organisations could be an issue for us as well.

CHAIR: Are there any further questions on this particular area? If not, I will move on to Mr Roberts. Thanks again for the demonstration that you gave us earlier today. I think just about everyone on the committee who saw that product that you have is thinking of children, grandchildren, nephews and nieces as excuses to go out and buy one themselves! Tell us, from your experience as a provider of these devices, about how the product is being utilised non-commercially and how widespread it is in Australia. Do you see issues relating to privacy breaches with the non-commercial usage of these devices?

Mr Roberts: The product that we manufacture and market is the second-generation product. We have been selling these products for four years. It is a connected toy, so it connects by wi-fi to a smartphone or a tablet. It is marketed purely as a consumer product, for the 14-plus age group. Australia is one of our largest markets globally for this product. We have sold over 500,000 globally. We do not get down into numbers per country, but it is a strong country for us, so there is a demand for this kind of product. As I say, we are in our second generation of product now. We have a large investment going forward in this category, so we have a lot more coming.

Predominantly, the easiest way to explain the product is, yes, it is flying quadrocopter, so it has four propellers, but it is really the extension, due to the smartphone and the tablet, of a remote controlled car or a remote controlled helicopter or plane. The difference is that now we can use the smartphone to control the technology, so it brings, in theory, the video game part of a smartphone. So just starting to talk, send text messages, taking photographs, playing music—the next step was playing video games from a smartphone. This is really how we came into this.

In terms of usage, it is marketed, as I say, as a consumer product for 14-plus. It is a toy, ultimately. Privacy wise, it has a 720p HD camera in the front, so you can record. You can take photographs or you can record video. It puts them back into the app and you can share these over social media. The privacy side of things—as with the use of a smartphone or a camera or a GoPro or whatever you are talking about, that is the responsibility of the consumer, the user. We put various disclaimers within the product, within the user guide, within the documentation online and also within the app. So there is the legal part of it there. On the privacy topic, from a manufacturer's perspective, we do not have any organisations coming to us. In theory, it would be the user of the product. Obviously, once it is in their hands, in theory, we have given a disclaimer as to their responsibilities and that is the same with health and safety and everything else that we are obliged to do. As a company, we do not run into privacy topics. Some countries, yes, because they have a stringent—some of the Middle East countries as an example—but here we do not tend to have this issue.

CHAIR: I am mostly with you on your argument that there is little difference with other remote controlled aircraft. But I will play devil's advocate for a minute. I could say there is a big difference between enjoying flying around a remote controlled helicopter in the backyard and flying around a device that is specifically designed to record images and then, through the app that you have developed, quickly upload them to the internet. That obviously poses a different set of circumstances regarding privacy to even a remote controlled helicopter strapped with a camera, because there is more difficulty in—

Mr Roberts: Yes. It gets back to the technology of the smartphone. The reason we did that is that that was basically what community concern was driving. With the first generation of product you could only stream live back to your device. We saw within a very short period of time after launching the product in 2010 that people were strapping cameras to our product. Our product is not designed to have anything strapped to it. It is not designed to take any weight. It is a very stable product. We saw people doing this thing that was affecting the stability of the product. Obviously, a lot of people wanted to record and wanted to share.

It is really the fact that we can do this over social media and over those platforms. Whether you are strapping a GoPro to a helicopter or something else, if it is controlled by a smartphone, which a lot of these products are—we are not the only ones now; we were probably the first, and we have really created this consumer sector that is

growing immensely—it is always the user's responsibility. In answer to the question, yes, obviously it is easier to do it with a device that has the embedded camera.

CHAIR: Are you aware of any sorts of serious instances utilising your product or similar products on the market in Australia where there have been quite serious breaches that have resulted in any sort of legal implications for the end user?

Mr Roberts: I have not had anything come across my desk that has implicated that. One would hope it is a common sense approach. There are disclaimers. Also, to put it into perspective, the product, as you heard this morning, is not discreet. It is not the kind of product where you could have it take off in in your back garden and fly it a few doors down, without somebody noticing it. You can hear it. So, in a certain way, one could say that you could do more with a camera on a stick or a GoPro or your smartphone over the fence, because they are covert, whereas this is certainly not covert. If the noise does not get you, the wind that it will create around will certainly cause attention. It is not designed as covert.

CHAIR: How good is the camera on the second generation device that you sell? How much can it pick up and from what distance?

Mr Roberts: It is a 27P camera. It is high definition. It does do a very good image—forward only; the downward camera is a low resolution.

CHAIR: From what sorts of distances?

Mr Roberts: It has a range of 50 metres. Obviously, the further you are away from the object that you are photographing, the more definition you lose. To get a good definition, you would certainly need to be at a distance of about five to 10 metres. If you picture how it was flying this morning, we did most of our flying horizontally. To start to get the good image from the 27P, you would have to hover and tilt the device that you are flying with at quite an angle to start to pan those sorts of shots. So you would have to be quite skilled and be there for a fair bit of time. Your battery would probably wear out within the 12- to 15-minute period.

CHAIR: Are images of individuals taken at a distance greater than the 10 metres or up to the 50-metres quite unable to be determined?

Mr Roberts: Yes, it is quite blurred.

Ms CLAYDON: In terms of your own market research, who would you say is buying your product? And do you have a mechanism for customer feedback?

Mr Roberts: Yes. This category that we have created is a bit like a cult; it has a big following. There is a lot of customisation of the product. We created an academy for the product where people can share their flights and their experiences. A lot happens on social media. We do have a mechanism of seeing—should people want to share that information with us—who is buying the product. I think it goes back to George's comment at the opening. We know that a lot of our consumers are 30-plus in terms of age. I think a lot of them are buying the product that they never had themselves or are just buying something else to use around their smartphone or their tablet. There is a large demographic. It is a 14-plus product. You seem to get a lot of parents, aunts, uncles or whoever buying the product for their kids or for their niece or nephew, which I think is quite negligible whether it is actually for them or for the kids. The demographic is really anything from 14-plus right the way up to 50-plus, which we have as well. It is a very large demographic. It is predominantly male, but there are also quite a lot of tech savvy, early-adopting females that use this product as well. It is a pretty vast demographic.

Ms CLAYDON: It seemed a very lightweight model that we saw this morning. If its uses are primarily outdoors, have had feedback in terms of accidents? I noticed there was a sort of rescue strategy button on the model this morning. I am just wondering if it often gets tangled up in coping with outdoor conditions.

Mr Roberts: You can totally rebuild the product. It does not matter if you do break a propeller; everything can be replaced. In terms of accidents, it has an indoor and an outdoor hull. The indoor hull is to protect the product and also the surroundings. Literally, with our product, like this one here, you could grab the propeller, put your hand straight in the propeller, and it would give you just a very small scuff on your hand—it would not do anything else—and the product would stop. As soon as any form of energy is placed on one of the propellers the whole product does an emergency cut-out. If you are flying—obviously you can't reach the product—there is an emergency landing button which will gracefully bring it down from its position. It is an automatic-land product anyway, so if you press one button it will land. The rescue mode is purely to manoeuvre the product out of a tree; it puts different power to different motors. It can be programmed as a 'bring me home.' For where we were flying this morning we could run a program that would get it back to point A, where we started from. In terms of accidents, we have had a few parents complain that their kids have done something with the product around the house. There is a disclaimer: you have to be responsible where you are using the product.

Mr DREYFUS: Are you aware of instances of people being injured in events involving your product.

Mr Roberts: No.

Mr DREYFUS: None?

Mr Roberts: No, not with the product. Whenever you fly one of these products it is impossible not to draw a crowd. As I say, we first showed this product in 2009 and there was a lot of feedback that this would never ever come to the market as a consumer product. Still today, all these years later, when you show this product you will draw a crowd wherever you are—everybody wants to see something fly. We will not do a controlled event to the general public unless we are in a netted area. When you see us at a trade show or a consumer show it is in a netted area, because originally people wanted to get really close—'What's this?'—and obviously we can't have that. Again, in a consumer-user environment the user has got to be responsible for where they are using the product. That is exactly the same with a remote control helicopters or planes, which have been around for 20, 30, or 40 years. It is the same ethos: the user needs to be responsible about where they fly the product. For us there is no real difference between remote control helicopters, which have been around in one form or another for 25 or 30 years, and a quadrocopter as a consumer product; the only difference is how you control it. The control is not an RF joystick; it is a smartphone. That is the main difference.

CHAIR: Mr Giuffre, do you want to give us an overview of how Voiceless is using this technology, and perhaps how other organisations you might know of may be using this technology, and how you deal with the privacy issues that emanate from the usage of that technology?

Mr Giuffre: Voiceless is a not-for-profit organisation. It is a think tank which focuses on raising awareness of animal suffering and factory farming in the commercial kangaroo industry. As a think tank we do not use unpersonned aircraft; however, we do see that there can be a benefit in the use of unpersonned aircraft in the animal protection space. We see that benefit in a number of ways. Firstly, surveillance provides the public with a degree of visibility over large-scale commercial agricultural facilities. At the moment there is a lack of transparency, particularly in factory farming, and, importantly, consumers are becoming more concerned about the way in which their food is produced and the conditions in which animals are kept within factory farms. In a sense, with that growing interest, it would perhaps be even in industry's best interest to start looking at ways in which their operations can be made more apparent.

As shown through countless undercover investigations, we have seen there has been serious cruelty, neglect and in some cases contraventions of the animal protection legislation which we have seen across the board in all states and territories. Despite this, there are inherent difficulties in regulators being able to monitor and enforce animal cruelty regulations, particularly within factory farms. Surveillance facilitates the effective monitoring and regulation of these industries, and what unpersoned aircraft provide that other forms of monitoring do not is that it is perhaps unannounced; it is generally unplanned—I would not go so far as to say that it is covert, but it does mean that unpersoned aircraft would be able to detect violations which could otherwise be covered up.

Surveillance itself can be provided as evidence in court proceedings, and can also be given to organisations or investigators like the ACCC, so complaints can be made against agricultural facilities that are not complying with animal protection legislation or are otherwise engaging in credence claims or misleading and deceptive conduct. We have seen the ACCC taking a more tough stance on credence claims in recent times' particularly claims about free range chickens and things like that.

Animal welfare, consumer protection, food safety, criminal justice—all of these issues are obviously incredibly important parts of public debate, and we believe that, particularly from a think tank perspective, this sort of surveillance opens the discussion. It provides a level of transparency. It gets the ball rolling, gets people talking. There is work by animal protection groups such as Animal Liberation New South Wales—the content that they have provided has sparked debate, and it is making people realise some of the cruelty and issues that are inherent in large-scale factory farming facilities.

For these reasons surveillance assists with reducing the rate of contravention of animal welfare regulations in our view, and it can be used not only by animal protection groups but also by enforcement arms like the police or the RSPCA in each state or territory, or the Animal Welfare League in New South Wales, to monitor and therefore enforce animal protection legislation.

From a privacy perspective, unpersoned aircraft are not intended to be used in the animal protection space to target farmers or to target individuals. I agree there is the issue of inadvertent privacy breaches; however, from my research—and similar to CSIRO's use of these aircraft—they are generally very low to the ground; around 30 metres or slightly higher. The camera is usually pointed down; so inadvertent privacy breaches would be incredibly unlikely.

Animal protection groups are really focusing on targeting animals on property and targeting corporations, and clearly those issues of privacy should not and ought not apply to corporations, particularly in the food industry, where people are obviously very concerned about where their food comes from and how animals are treated in that production process. From my perspective, industry groups that are concerned with the use of unpersoned aircraft ought not be; they should look at transparency as being a good thing for industry. It should only be a concern for industries that are not doing the right thing.

CHAIR: So specifically you would be an advocate for non-government authorities, not-for-profit organisations and civilian activist groups having the right to use these drones, to go in and inspect what you think may be breaches going on?

Mr Giuffre: I think that this sort of technology is important in the monitoring and enforcement of animal protection legislation. So I think that it can be used not only by civilian groups or not-for-profit organisations but can also be taken up by enforcement agencies like the RSPCA, state and territory police departments or the Animal Welfare League in New South Wales.

My concern in restricting its application to only enforcement agencies is where do we draw the line. Does it mean that we would start thinking about all forms of photography on agricultural facilities as being no longer permitted? I think it is important to recognise that what this sort of surveillance could do for public debate, what it could do for transparency, what it could do from a consumer protection perspective and also what it can do from an animal welfare perspective—and I think the industry should embrace the technology.

CHAIR: You mentioned earlier that corporations should not have the same privacy protections as individuals. But the nature of farming is such that most farms have company structures in some way, shape or form—they may be farming families but have a company structure, perhaps even with shareholdings in that company—so where do you draw the line there in terms of who has the privacy protections and who does not?

Mr Giuffre: I tend to take the view of the High Court in ABC v Lenah Game Meats, which said that corporations generally should not be given the sorts of privacy protections that would ordinarily be given to individuals. It is about protecting individual dignity, and corporations should not necessarily have the right to have that dignity protected—particularly when it comes to food processing, in my view. It is an incredibly important part of consumer protection law that individuals are able to know where their food comes from and how the animals are treated. Where do we draw the line? I think there needs to be a balancing act. We need to weigh up what the benefits are to the community and what the potential detriments would be to the individual whose privacy could be violated. Following that balancing act, I firmly believe that un-personned aircraft could provide significantly more benefits to the community, to consumers and to animal welfare than potential breaches of privacy.

CHAIR: But you do accept that to fly one of these aircraft in the airspace that is very close to ground level and to take images of what is essentially private property is a breach of privacy?

Mr DREYFUS: Why? That is a leading question. But perhaps I should let Mr Giuffre answer it as he has already referred to ABC v Lenah Game Meats, in which the High Court held very directly that privacy is a human right; it is not a corporate right. That is what the case turned on.

CHAIR: But is it a breach of privacy even for the landholder, whether it be a company or a person?

Mr DREYFUS: It is not a breach of privacy. There is no privacy obligation owed to a corporation. In fact, for those who are not familiar with ABC v Lenah Game Meats—it was a case concerning animal rights activists breaking into a farm in Tasmania. You probably know, Mr Giuffre, what type of farm.

Mr Giuffre: A possum farm.

Mr DREYFUS: A possum farm in Tasmania. And the suit went to the High Court on the basis of an invasion of privacy but the case was dismissed on that very basis: because the right to privacy does not belong to corporations; corporations are not people.

CHAIR: Okay. The member for Pearce?

Mr PORTER: I certainly agree with what was just said with respect to the ABC case, but, nevertheless, it seems that at least there is the potential for a breach. We are not talking here about inadvertence; we are talking about the explicit use of civilian surveillance. Again, looking at all the different jurisdictions that have statutes pertaining to the use of listening devices for optical and audio recording, it would seem to me that the type of civilian surveillance that you are advocating would require a fairly substantial change in a range of existing statutes to make lawful the use of an un-personned vehicle to fly over and record activities that may fall inside a definition of 'private activity' whether that property was owned corporately or privately. It seems to me that that

could potentially be in breach of a whole range of state statutes that pertain to listening devices—understanding the issue about civil breaches of privacy, it nevertheless may be unlawful.

Mr Giuffre: To be honest I would not be able to tell you the specifics of the legislation in each state and territory. In saying that, from my research in New South Wales it does not seem as though the usage of un-personned vehicles in that state would breach legislation—but that is on my very preliminary view. It seems to me that the law is unclear in this area.

Dr STONE: I am assuming, Mr Giuffre, that by definition of the purpose of your surveillance you would never seek permission or speak to the owners of the property, whether they were a corporation or a family property. It would be part of your activity to be there without them knowing you were coming.

Mr Giuffre: Just to clarify: Voiceless would not be undertaking this sort of surveillance itself. We are merely participating in this from a research perspective.

Dr STONE: From a theoretical—

Mr Giuffre: From a theoretical perspective.

Dr STONE: But, theoretically, though, you would not envisage that you would be letting the place to be surveilled know that you were coming.

Mr Giuffre: I believe there could be a variety of uses for unpersonned aerial devices. I could foresee it being used, for instance, by the RSPCA where an agricultural facility could be notified that a drone would be used to survey the area. So it could be announced, unannounced, planned or unplanned. But I do not believe that the current uses of unpersonned aircraft is covert.

Dr STONE: So, where the police in fact have to have warrants to enter private property to undertake an inspection or an examination of what is going on, you would not see that in a similar vein—that there would need to be similar application to someone in authority to have access to this information, that it would need to be a legitimate agency of some sort in terms of law and order?

Mr Giuffre: Sorry, would you be able to repeat the question?

Dr STONE: I am saying that, if the police want to come and look at what is going on on my property, they need a search warrant. And they need to apply for that through a magistrate. You are suggesting that, if you are an NGO whose charter was to find animals being starved in a feedlot, for example, you would not envisage that there was the same sort of need for a warrant to be executed so you could go and see what was going on?

Mr Giuffre: I have not considered the specific details around how an enforcement agency would be able to use an unpersonned vehicle. However, I do see that there could be benefits in using drone technology in an unannounced, unplanned way.

CHAIR: Are you aware, though, of animal rights organisations in Australia that are currently using this technology for the purposes about which you are talking?

Mr Giuffre: There is one organisation in New South Wales that I understand is presently using it—only through media reports. That is Animal Liberation New South Wales. I am unaware of any other organisations.

CHAIR: I want to go back to the question again, and let me strip out the difficult part of it—the corporations part—and talk about the family farm, owned by one or two individuals. You would accept that it is a breach of their privacy to bring a device onto the property and essentially spy on the activity that they are undertaking?

Mr Giuffre: I don't accept that. From my research, the way that drone technology is presently being used is on large commercial facilities and merely to survey the area where animals are located on farmland.

CHAIR: Would Voiceless be an advocate for an activist organisation to go in and film something and then have that broadcast through television or social media, YouTube or whatever, if the incident was maybe not illegal but something that the organisation might think is ethically wrong and that they think the public would think is ethically wrong?

Mr Giuffre: Voiceless strictly does not endorse unlawful activity of any kind. So Voiceless does not endorse, and would never endorse, the kind of trespass you are referring to. In saying that, if footage emerged that showed, for instance, animals being subjected to cruel or indecent behaviour, or there was a violation of the animal protection legislation, then that footage should be given to authorities for enforcement purposes.

CHAIR: Okay. You just said that you would not encourage the unlawful use, but what I am talking about is what you are advocating—that is, the ability of civilian organisations, activist organisations, to use drone technologies in going onto farms and taking footage or photos.

Mr DREYFUS: I don't think that is quite a fair characterisation.

Mr Giuffre: No, it is not.

CHAIR: It is a fair characterisation—

Mr DREYFUS: He has just said that the policy of the organisation is to not endorse unlawful conduct, including trespass. Perhaps you could confirm that, Mr Giuffre.

Mr Giuffre: Absolutely.

CHAIR: This is the prime thing that you are advocating for—

Mr Giuffre: No, what we are advocating is that the use of drone technology could be very effective in the monitoring and enforcement of animal protection legislation. We believe that—

CHAIR: Would that be staffed by civilian organisations?

Mr Giuffre: It is currently being used by civilian organisations. I started off by saying that it should also be used by enforcement agencies like the RSPCA, the Animal Welfare League and the police. If it were to be used by civilian organisations—and, as I said, we do not endorse the unlawful use of technologies like this or the unlawful trespass on private property—within the confines of the law then it could be incredibly effective for a number of reasons.

CHAIR: I will go back to my scenario again. An animal rights organisation utilises material, which was perhaps gained through lawful means somehow, from drone technology footage that has been captured of something that they believe is unethical but perhaps is not illegal. Would you endorse the use of that material going on YouTube, television or whatever to raise the plight of that cause?

Mr Giuffre: If the material was obtained lawfully, and it showed that animals were treated cruelly or indecently, then of course I believe that that footage should be provided to the public. This is because I believe that consumers and the general public have a right to know how their food is produced and how the animals are treated in factory farms.

CHAIR: I am going to pose an extreme example, which I think directly correlates with this. Someone has footage taken using drone technology of a man and woman, who is not his wife, engaged in a romantic liaison and posts that to the internet. It is not unlawful but it is unethical—

Unidentified speaker: Perhaps it is not illegal to actually show it.

Mr DREYFUS: Is the liaison unethical, or—

Ms CLAYDON: Or the photography!

Mr DREYFUS: But seriously—

CHAIR: I am asking a serious question. You basically said you would advocate for images that you would deem to be unethical but may not be unlawful to be broadcast publicly, where the footage may have been captured without the landholder's permission. How does that square with that other scenario that I talked about?

Mr Giuffre: I do not really want to engage in hypotheticals in that sort of situation. I say again that, from my perspective, if there were footage to emerge that was lawfully obtained that did show animals in cruel environments or in conditions that in our view seemed cruel or inhumane then we believe that that footage should be dispersed to the public so that people have can know where their food comes from and how the animals were treated.

Mr PORTER: I am interested in the clear distinctions between tortious notions of privacy, criminal and civil issues of trespass and then recording. My own observation of some of the issues here would be that there is a great distinction between a drone that has a camera and one that has not. Without a camera there may be issues of trespass; with a camera you enliven the issues pertaining to recording. In most jurisdictions there are laws pertaining to where you can and cannot use recording device, either optical or audio. It seems that there is very high potential for a breach of those laws by civilian surveillance—for whatever purposes; however well-meaning and well-intentioned. That is issue No. 1.

When you say that you are unaware of whether or not, and would never advocate the breaching of the law, it does seem to me at least that some existing laws carry a very high probability of breach with the sorts of scenarios that we are describing. So I am trying to elicit a view on whether or not those laws, in the view of an organisation like Voiceless, need to be looked at or changed.

The second thing is: what are the difficulties that an organisation like Voiceless sees with alerting non-civilian organisations that have the ability to investigate breaches of statute or other breaches and allowing investigation by them rather than by civilian organisations? Thirdly, when law enforcement agencies do surveil, they have a standard, usually based on warrants, and the standard is, generally speaking, a reasonable suspicion of unlawful

activity. It seems that what you are talking about, with respect, is an information-fishing exercise, not based on any reasonable suspicion or what would otherwise formulate the basis of a warrant. So can I just get your comment on those issues.

Mr Giuffre: On the first point, as I said before, if drone technology can be deployed in a legal fashion then I believe that it should be used for enforcement and monitoring purposes. Secondly, I do believe that, if material is obtained and that material reveals that there is cruelty or a potential violation of animal protection legislation, of course it should go to enforcement agencies, but of course it would be up to the enforcement agencies to pursue that and make sure that the animal protection legislation is properly enforced and that, if cruelty is found, appropriate penalties are imposed on that facility or that operator. What was your third question?

Mr PORTER: My second question was: why not leave investigation to bodies statutorily empowered to investigate?

Mr Giuffre: Absolutely. I agree. The problem at the moment is that there are difficulties in the monitoring and enforcement of animal protection legislation, to the point where we are now seeing that cruelty goes on unmonitored, unchecked and unenforced. Voiceless's position is that there needs to be a strengthening of the monitoring and enforcement of animal protection legislation.

Mr PORTER: And this leads to the third question, which is that perhaps one of the deficiencies that you are seeing or alluding to is the fact that a law enforcement agency, before it can engage in surveillance of the type we are describing, is going to have to apply for and receive a warrant based on a certain standard. Civilians who surveil are not going to have to do that. You could, based on the scenarios that we are talking about here, use an unmanned vehicle to surveil a property based on a hunch. Is that something that would be advocated?

Mr Giuffre: It would be difficult to determine, I think. From my perspective, the only reason why unmanned vehicles are being used at the moment is that there is a clear deficiency. I would perceive that a lot of the cases where animal protection groups would come and survey would be where they were operating on more than just a hunch, where they do have material and where they would have evidence of a breach.

Ms CLAYDON: I just want to go back to some of the applications that you were referring to, because I could see that there might be a range of farmers, for example, who are engaged in biodynamic or organic farming, who are selling their produce on the basis that they have free range available and who might wish to use this technology as part of a monitoring system to show that they are adhering to particular industry standards and guidelines. Is that currently the case? Are there any particular individual farmers or perhaps umbrella organisations representing those types of farming that are using uncrewed or unpersonned aircraft to assist in the monitoring of adherence to those standards?

Mr Giuffre: It is a really good point. I am not aware, but I believe this is the perfect area where industry could be using unmanned or unpersonned aerial devices to be able to show their compliance with model codes of practice and prove their claim that their products are, for instance, free range. I think that it is an excellent area for industry to be able to use this technology to provide more transparency in where our food comes from and how animals are treated within these facilities.

Mrs MARKUS: Just quickly, you mentioned Voiceless would not use unmanned aircraft. Would Voiceless engage a third party?

Mr Giuffre: We have not previously and we do not plan to in the future.

Mr PORTER: That dovetails into this: if the AFP uses an unmanned vehicle for surveillance purposes is that usually subject to a warrant?

Cmdr Harrison: We do not use UAVs for surveillance purposes.

Mrs MARKUS: If you did, would you need to have a warrant?

CHAIR: We might go straight into that now and you can give us an overview about whether you might be using them now, whether there are plans for the future and how you are managing the privacy issues as well.

Cmdr Harrison: Our use of UAVs is extremely limited. We currently use UAVs to image crime scenes where it is lawfully under a warrant, so we have a lawful authority to be present there. In addition to that, it is just a further extension of the normal imaging that we would do at the scene. The imaging is undertaken by our own trained staff from the forensic area, and these would be the people who are trained to operate both the imaging equipment and the UAV. The UAV itself is a quadcopter, so it is a rotary system—very small, just under two kilograms—and the model itself is from a company in Canada that supplies other law enforcement agencies around the world.

A typical example would be last year, when the AFP assisted New South Wales police at their request under warrant for a search for the remains of Donald Mackay on a rural property. We assisted in the imagery and the recording of that search and excavation. The UAV provided a different and unique perspective to aid and assist in that process.

One could perhaps visualise the AFP's use of the UAV as no more and no less than how one would use a static cherry picker, which is what we previously have used. For expediency, cost effectiveness and mobility the process we now undertake is with the UAV. The UAV is overt. It is operated by uniformed personnel and it flies within the CASA regulations—that is the sub-400 feet regulations—as well. It is not a point-to-point in the way it is used; it is very much a flight, a hover, a record and then return to ground.

The imagery itself is governed by the standard procedures of any imagery that the AFP would record that is seen, even more so. The Nikon SLR camera that is used for the ground-based recording scene is fixed to the UAV, because that is just a platform, and that camera is used to continue the recording from a different perspective. The imagery and metadata are then dealt with in the same way under the same rules, regulations and authorities as all other imagery that we would use in our investigations. That is our current use of our UAV.

CHAIR: Planned future usage, expanding more into surveillance or anything in this area, or no?

Cmdr Harrison: We have no plans, research or current activity into surveillance. If that were the case, that would clearly be done on the current lawful authorities. We are currently exploring the benefits and opportunities for search and rescue and for missing persons; we can see some benefits there. We are not undertaking any operational activity in that space, but that is where we see the immediate future opportunities to benefit the community.

CHAIR: You probably have knowledge of your state counterparts. Do you know how they are utilising drone technology?

Cmdr Harrison: I am aware that other states and territories do use UAVs. I am not familiar with the detail of that. It is my understanding that the Queensland Police are the most mature and extensive in their use of UAVs.

CHAIR: I will throw it open to questions from other members of the committee.

Mr PORTER: I might use that as a base to put another point to you. This is just an observation, but it seems to be that what Voiceless would advocate is the use of a civilian surveillance device, a UAV, without any form of warrant. It seems to me that, no matter how well intentioned the use might be, it is a very strange outcome if trained professionals in law enforcement are required to satisfy an independent person, usually in the judiciary, of a reasonable suspicion of some kind of unlawful activity to then be able take a UAV into property, whether it is corporately or privately owned.

Mr DREYFUS: Just before that question is answered, can we ask Commander Harrison: were you to use a UAV for covert surveillance, you would be required to get a warrant?

Cmdr Harrison: Absolutely. It would be not different to any other intrusion into that sort of area.

Mr Whowell: Can I add some detail to that. We have to comply with the Commonwealth Surveillance Devices Act. It has quite a broad definition.

Mr DREYFUS: I am just trying to unpick what bit of law we are going to insert. It is the Commonwealth Surveillance Devices Act.

Mr Whowell: Yes. Based on the existing law, we would have to look at what the application was going to be and whether that fell within the definition of a surveillance device, which, from memory, is very similar to the versions you have put on the table today. Then we would have to look at the application. Potentially, yes, that has a three-year threshold for an offence and, if there is trespass and the intrusion is in privacy in that sort of test process, you would have to seek from a magistrate—absolutely.

Mr DREYFUS: So covert use of a camera is a surveillance device requiring a warrant?

Mr Whowell: Cameras are quite difficult, if you are talking about public spaces and that sort of surveillance, because my understanding—and I can be corrected by others who know better—is that if it is in a public space you do not need a warrant for that.

CHAIR: But if it is on private property—

Mr Whowell: If you are installing a device where there is trespass and in that private concept of a private home or business, absolutely—

Mr DREYFUS: Totally. There is no doubt about physical trespass issues; they will always require a warrant. I am just trying to pin down what it is about the use of a UAV, which does not involve physical—

Mr Whowell: It is too theoretical for us, because we have not turned our minds to it. I am trying to think of a scenario that we could use in a public circumstance, and, I am sorry, I cannot at this stage. We might be able to deal with that separately.

CHAIR: Mr Giuffre, do you want to make a response to the member for Pearce's question?

Mr Giuffre: Yes. As long as the use of the UAV is lawful, I believe and Voiceless believes that it could be incredibly effective in monitoring agricultural facilities—as long as that use is lawful.

CHAIR: Any further questions to the AFP?

Dr STONE: If I could, Chair. Obviously, the cameras that we now see in malls and streets all over the place are taking photos. That photography can be used as evidence, I understand, for a crime that might be committed and captured on the tape. Is there any similar sort of circumstance where one of these little unmanned vehicles can be used to go up and down a mall, doing a similar sort of thing? Is there any comparison there with how they might be treated in law? I mean, one sticks to a pole and one does not. Other than that, they are in a public place; they are looking for crime.

Cmdr Harrison: It is not something that the AFP has turned its mind to. The fixed use of closed-circuit television is reasonably well established and the laws governing it. One would assume that it would be governed by the same regulation in that same space, but it is not something that the AFP has turned its mind to and is actively considering.

Dr STONE: I am thinking of a football crowd or some other place. It might a big demonstration somewhere where you are wanting to keep an eye on a crowd and make sure someone is not about to be hurt or someone is not committing an offence.

Cmdr Harrison: Certainly, other nations in law enforcement do use UAVs to aid and assist them in the public safety monitoring of such things.

Dr STONE: I believe that they have been used recently to surveil crowds in Bangkok, Thailand.

Mr DREYFUS: Do you know what the Queensland Police Service are doing with their UAVs?

Cmdr Harrison: Not specifically, no.

Mr DREYFUS: Do you have any idea? You said that they were the most advanced. I am just curious to know what they are doing.

Cmdr Harrison: My advice is that they are the most advanced and mature, but I do not have any information on the nature of that.

Mr DREYFUS: Do you have any examples of uses by state police forces of UAVs that you are more closely familiar with?

Cmdr Harrison: No.

Mr PORTER: Going to that, one of the things that I have heard of as a possible present application is the use of UAVs to cover large areas of ground looking for things such as marijuana crops and so forth, and that does enliven the question that Mr Dreyfus asked. Presumably the first port of call for law enforcement in that circumstance is going to be the surveillance devices act of the jurisdiction, which may have issues around warrants or other exceptions for law enforcement against a prima facie offence of unlawful use. I know it is a general question, but would your first port of call be the Surveillance Devices Act?

Mr Whowell: Yes, absolutely. If there were a search warrant in place and things like that across the property, you would have to see whether the warrant gave you that power or whether you would need to get a surveillance device warrant as well. It would depend on how you received—

Mr PORTER: Or whether there was an exception under the act.

Mr Whowell: Yes, absolutely.

CHAIR: Ms MacTavish, do you want to buy in on this?

Ms MacTavish: Boy, do I! My career began literally in research and development of gathering, retrieval and assessment of satellite data, working closely with the federal government and the RCMP in Canada. If I could go right back to the very beginning of this session, even in mining, regardless of your altitude, I beg to differ about what kind of information can be gathered. You can certainly gather very detailed information. With respect to surveillance and warrants, I think we may need to remember and consider the fact that, when we take a look at what is legal or not legal—and I am not a lawyer—we have wrestled with understanding who owns the airspace.

So do you need a warrant to occupy airspace over private property? That property may be yours, but who defines the airspace and ownership? Certainly CASA comes into play over 400 feet. However, below 400 feet we have to begin to consider that.

We also have to consider the fact that an unmanned system that is being operated by either a person or an organisation that has an operator's certificate can only be in that space if they have area approval from CASA, so whether or not they should be there should be present and known based on their ability to be there, and that is because of their operator's certificate with CASA. Let us say they breach that or have special dispensation from CASA to operate above 400 feet; you do not know that either. So there is a lot that comes into play with respect to this aspect of surveillance, warrants and what is legal or not legal. It is pretty messy, but we are working towards understanding that and making it so that the commercial aspects that we want to be legal are legal and are defined and so that we enable an industry.

CHAIR: Are there any questions following on from that?

Dr STONE: Yes. Remember the question I asked about commercially confidential information and the potential for industrial spying, as I will call it, to put the common term in place. Are you looking at that too? Are you aware of any of that sort of movement internationally for people to be concerned about what might be looked at—someone's stockpiles of whatever or how they are organising manufacturing in a certain place or even occupational health and safety issues on a big building site? Are you aware of any of that sort of conversation going on about what might or might not be lawful in terms of someone else surveying an area that they do not have permission to cover?

Ms MacTavish: Yes, absolutely.

Dr STONE: So where are you going in terms of that discussion?

Ms MacTavish: With respect to unmanned systems, it again comes down to enabling an industry to operate commercially and legally. If you want to take the example of stockpiles in mining, it is a known fact and it is easy for any country to take a look at any stockpile in any other country using satellite information. It has been around forever. So you know what? Put a tent over it if you do not want them to know. It is not common sense from the general public's purview but it certainly is for those of us in the industry who understand the technology, so when we are talking about this association trying to enable industry in this country it is about true commercial operation for industry. Yes we do look after military, academia, government—everything, but really what we are trying to do is enable, and that goes back to what I spoke about earlier this morning, which is setting up the infrastructure in such a way that we have a viable industry. We cannot take off and start to operate without having the laws, without having the regulatory things, in place. That all comes into play in this aspect.

CHAIR: I am going to move on to Mr Corcoran. Sorry to keep you waiting—it is probably one of the more in depth ones so we are going to extend our session to thrash this out. I suppose this may also be another controversial area involving privacy and the usage of this technology by the media so I am just wondering, given your expertise in the field, what current applications are there for drone technology within the media, what do you see developing and how do you think the privacy issues which are always pretty tricky when it comes to the media anyway are going to be resolved?

Mr Corcoran: I will come to the current applications in a minute, but just starting with the range of research and what we have been looking at—and I speak as a private individual not representing ABC policy today—we have basically been looking at everything from the concept of the disposable drone, which is the small consumer grade technology, as a safety and reconnaissance device. When we have got people in places like Afghanistan, the ability to look over a hill provides safety, and it is the same with covering disasters—what is around the corner, is a bridge intact; that sort of thing. That is at the very smallest level. The next level being looked at is probably the space where the majority of drone news gathering would take place, and that is with the multirotors weighing between 1.5 and 7 or 8 kilograms. Talking to the cameramen and other experts in that area, that is the sweet spot at the moment. The bulk of news gathering and indeed media work that is undertaken at the moment is conducted by platforms of that capability.

Then at the other end of the scale we have also been exploring the very large tactical level drones which are now commercially available. These are for military use—things like ScanEagle and Aerosonde. These are craft with a capability of 24-plus hours in the air; they have a three- or four-metre wingspan and cost probably one tenth the acquisition cost of a typical news gathering helicopter. They would have a range of capabilities that are quite useful. We are keen to explore further opportunities with emergency services, particularly with things like bushfires where you can put one up in a racetrack pattern over a fire for more than 24 or 26 hours day or night. That could also assist in the ABC's obligation as the emergency broadcaster. You could live stream this video;

you could put in modules that act as a flying cellphone tower when communications are down. It could fill a range of functions. That is one example.

With the larger drones—you can call them a lot of things but I will call them drones—such as Aerosonde and ScanEagle, they are also now developing commercially available technology where they can be controlled over the horizon by satellite, where you can get vision feedback. You have a capability of ranging many hundreds of kilometres away from your point of launch. So there are stories there. Things like the clashes between whalers and environmentalists in the Southern Ocean could be independently verified. We could see what is happening with asylum seeker boats 300 kilometres over the horizon. It gives you the potential to independently verify those issues. There is searching for lost bushwalkers. That is the top end of the technology, and probably the sort of thing that only major media groups like the ABC or commercial stations, who already operate helicopters, could look at. Again, I think the bulk of potential use is in that 1.5 to seven kilogram multirotor category.

Given the current CASA regulations, we are not seeing a lot of what you would define purely as news gathering, basically because of the restrictions that are in place in terms of operating height and that sort of thing. What you are seeing—and the ABC is included in this—is this technology being used when we hire one of the 60, 70 or 80 approved operators for documentary filmmaking, sporting events or that sort thing where it is a clearly defined preplanned operation in a set location. A good example was just here in Canberra on Australia Day. The ABC events unit covered the Australia Day flag raising ceremony. That is an outside broadcast that goes national every year. They had multiple cameras on that event, and this year that included a UAV—a multirotor—which was very successfully integrated safely with planning and CASA approval. So, it was quite a significant event.

In terms of the commercial stations and the ABC, we are seeing current affairs programs use the technology offshore, dependent on the jurisdiction where they are operating. Internally, ABC programs such as *Four Corners* have used hired contractors who fly the multirotors for set-piece filming in the range from ground level to 400 feet, which is terrific. That is an area which is the main game for filmmakers, and their helicopters cannot always provide that. So this provides a very cheap and highly effective alternative. Cameramen call it the equivalent of operating a 400-foot-long jib or a 400-foot-long camera boom because that is the space you can operate in and that is where they have been working. However, under the current restrictions we are not seeing a lot of news gathering yet, but we will see what happens when the rules change.

CHAIR: But there are obviously no restrictions if an application to have a device floating around suburban neighbourhoods to actually operate in that airspace is approved. As long as the application that went to CASA abided by all of their operational and concerns, you would get the tick off on that. What I am getting at is that there is capability for media organisations to actually have drone technology in suburban areas picking up footage for them.

Mr Corcoran: That is an issue, and this is absolutely a surveillance technology, but I would argue that there are an equal number of other new technologies available that are equally invasive. What it comes down to is: first of all, abiding by the law; editorial judgment, and if you work for a major media group there are in-house editorial guidelines—in the case of the ABC, they are fairly rigidly imposed—; and ethical considerations. It is a matter of factoring all of those in on the importance of the story, the location and safety. All these things get factored in, as they do now. This provides a phenomenal capability, but there is a lot of new technology out there already.

People were alluding earlier to the concept of what constitutes a reasonable expectation of privacy in this current environment, particularly when you have drones in the equation. Say you are flying up to the fifth floor of a flat in Potts Point in Sydney, do the same rules apply if you are filming a farmer on his veranda out in Dubbo? What are the rules? We do not know. It is almost like the barbeque question: who owns the airspace 10 metres above your barbeque? This is a debate they are having in the United States at the moment. There are just so many grey areas with this which certainly need defining.

In terms of privacy, I would argues that, with some modification, the current privacy provisions regarding media use are sufficient. I do not think we need a whole raft of new privacy rules and regulations on media use of drones. I think where we have a problem already is that state by state there is whole patchwork of different laws that we already have to abide by in terms of surveillance, trespass and a whole range of other related laws. Perhaps it would be good if we could have some uniformity on that. That would help.

CHAIR: You mentioned other devices which could be equally intrusive in terms of surveillance. Could you list some of those devices that you are talking about?

Mr Corcoran: Camera technology, long lenses—the capability now is that you do not need to be that close. With the filming capabilities that you have from current generation news helicopters as well—with the stabilisation mounts and the technology—they do not have to be that close. The technology is there. There are the

capabilities for things like smartphones; every smartphone has a camera on it. I guess that gets into that whole area of freelance drone journalists and the potential for people just chancing on something and wanting to do it. But I think that is a slightly different issue as to how major media groups would operate, and are operating today.

CHAIR: So with that answer, I probably do agree with you. But I will play devil's advocate a little bit. You mentioned the helicopters are expensive to buy. They are expensive to get up in the air to fly around too. For a filming exercise, whether it is a long-range, an iPhone or a digital camera, you are not going to be able to get that camera to zoom in on someone's fenced backyard unless you are up at a great height, like in a helicopter. So, obviously, the drone technology would allow a media organisation, like a current affairs show, to go in and do the kind of sensational stuff that they do, but in even someone's backyard. Could you see that happening? Do you think there are issues with that?

Mr Corcoran: Well, I would argue you already have that issue anyway. That exists even without a proliferation of drone technology through the media, and some media groups use them. Yes, potentially it is an issue; but we are not there yet. As part of my research I looked into the potential use by paparazzi. When we talk privacy, particularly in the States, that is the first issue that people raise. I looked at some highly publicised cases of paparazzi use, one in France and one in Bali. But on the whole the top paparazzi have not really embraced the technology yet. I do not think there is any altruism there. I think it is simply because the platforms are not good enough and their whole industry is based on the stolen moment. The technology cannot carry the big lenses and cannot get close enough. But that kind of media use and media operations have always been there.

CHAIR: Do you have questions on this particular aspect, the media aspect?

Mr Dreyfus: Mr Corcoran, leaving aside drone technology, you are suggesting that the technology is there in a whole range of ways right now; just putting a camera up in the sky somewhere or in the air to take particularly intrusive images.

Mr Corcoran: Yes.

Dr STONE: And listening devices I expect?

Mr Corcoran: But there are laws against listening devices. There is a whole range of different laws in different states. That is where I think some of the media lawyers get sent grey before their time, trying to figure that out on a state-by-state basis. All I can say is that for the major media groups, a lot of this comes down to editorial judgement.

There was some discussion earlier about whether they should employ some system that will pixelate faces, that kind of technology. For our purposes, obviously, I would argue against that. It comes down to a judgement. It is a call by the editorial team. Do we publish? Should we send our reporter or our team into this property? Does the story warrant it? All these factors are in play on every major story. There is absolutely no doubt that this technology is extraordinary. It enables people to get shots previously only available by helicopter. This is with the small operation. At the big end of the scale, for companies that operate news helicopters, I do not see it as a replacement for news helicopters; I see it as supplementing the coverage, and it is not cheap. With the platforms I was talking about earlier—about their being put over a bushfire or put out over the Southern Ocean or the Timor Sea—you are looking at, with all the gear on board, probably $350,000 just to buy. But that is still one-tenth the cost of a news helicopter, so it depends which point you want dip in or out of the debate.

Mr DREYFUS: Perhaps just to flesh that out a bit, to pick up Ms MacTavish's point from before—you can identify a face from a satellite image, and you can sit on a hill 10 kilometres away with a very big telephoto and get some spectacularly sharp images, but what this small drone technology potentially allows is getting up really close, very cheaply.

Mr Corcoran: Absolutely. And the term 'drone', although it encompasses everything from a $50 toy to a $200 million US military surveillance platform, in terms of media use, if we put aside some very sensible regulations that we have in place at the moment from CASA—and I know they are working on reforming that—if you put aside the regulation for the moment, you are really only limited by your budget and your imagination. It is already out there. And I think that the problem is that the technology is now progressing at such a rate that regulators and legislators risk being buffeted in the slipstream in this stuff. I have been following this for only a couple of years, but I have trouble keeping up with the capabilities, and every 18 months it seems the capability doubles and the price halves.

Mr DREYFUS: My experience is that the media are very imaginative and not very good at self-limiting, either. So 'limited only by the imagination' does not suggest much to me in the way of limitation, once the technology enables almost anything to be done. Do you think that the media are likely to self-limit in this area?

Mr Corcoran: I cannot speak on behalf of the entire media.

Mr DREYFUS: I am not asking you to.

Mr Corcoran: It depends; it is the same situation that we have at the moment. You have media groups that have fairly stringent in-house rules—they not only abide by the law but have their own in-house rules. You have others that have different interpretations of what constitutes a news story. I do not see that changing. What I see is a capability being placed in the hands of people, and you still have to make value judgements on how to apply and use that.

Another big issue for me is safety. The whole starting point for this project for me was safety, having worked in places like Afghanistan and Beirut. What can we use? Can we deploy this technology—exploit it—to improve our coverage and to improve the safety of our people? A lot of journalists get killed doing their job, and that is another big aspect for me, and that was actually my starting point with this project. But it is not really a domestic privacy issue.

Mr PORTER: I take your point about the divergence of surveillance devices legislation between the states and the Commonwealth, but it seems that almost all the state and territory jurisdictions have got something in this space and the Commonwealth has something in this space and, leaving aside that fascinating issue of trespass and whether or not the physical presence of a UAV in an airspace constitutes a trespass, it seems that the essential principle around surveillance—whether that is audio or optical, as this is—is that you cannot do it lawfully in circumstances where those people being surveyed optically or audio recorded would reasonably expect not to be optically or audio recorded. So, whether you are over a farm or at the window of a 40th-storey apartment, the basic principle is that it is unlawful to visually record those people if they would reasonably expect not to be recorded. And there are certain exceptions to that, whether they are by warrant or by other statutory grouping exceptions or consent or disclosure or whatever. Whilst the technology is enlivening that issue further and further with UAVs, do you in your research have a view as to whether or not that essential principle is the correct principle to be applied for legislation, however it diverges in detail?

Mr Corcoran: I do not have any legal qualifications.

Mr PORTER: It is a philosophical question.

Mr Corcoran: I think it is reasonable. Going back even in further, what constitutes a reasonable expectation of privacy?

Mr PORTER: That changes with the technology, one would posit.

Mr Corcoran: Yes. I do not have an answer. Again, coming back to current practice, how we operate varies from state to state—

Mr PORTER: Indeed.

Mr Corcoran: and from story to story. Sure, every media group in the country would be happy to see some sort of uniformity there on that.

Mr PORTER: Indeed, but I guess in 1920 you had a lower expectation of being able to be recorded through a 40th storey window than you might in 2014. My view of the legislation is that it is clunky in terms of the way in which it is dealing with this technology.

CHAIR: Are there further questions to Mr Corcoran?

Ms CLAYDON: I just wanted to follow up. I actually got to see first hand the use of this technology in a sporting event back in Newcastle, where there was an international surfing competition. It was pretty amazing the kind of footage. I can see that application being very useful there. Given that you are not advocating, as I understand it, for any additional privacy laws with regards to media operations, have you in your call for uniformity between state and territory laws actually put forward anything?

Mr Corcoran: No, I have not.

Ms CLAYDON: A wish list?

Mr Corcoran: A wish list, basically, yes.

Ms CLAYDON: Thank you.

CHAIR: Dr Mejias Alvarez, as you started, I am going to ask you to conclude. After hearing all this, and given your expertise in the technology, do you believe there is a need for some greater regulation regarding privacy or at least looking across all jurisdictions and getting some nationalised system?

Dr Mejias Alvares: The short answer is yes. Moreover, on a personal reflection, unmanned aircraft were a big player at the last consumer and electronics expo in United States. What are the implications of that? We are talking about an industry that releases a new smart phone, a new tablet, a new laptop, a new video console every

six to 12 months. It is an industry that moves fast—smaller devices, more powerful with longer lasting batteries. The fact that unmanned aircraft are now part of that industry, personally, I see a future that we may have new unmanned aircraft every six to 12 months—smarter, perhaps smaller and with longer lasting batteries and with different levels of autonomy, ranging from small toys to more advanced and more intelligent aircraft. If I can provide my own view of the industry, the technology is here and we need to start thinking of embracing the technology and perhaps focusing on defining the guidelines for its responsible use—a code of conduct, perhaps, and regulations for the safe use of the technology. That is my personal view.

CHAIR: Thank you very much for everyone for participating in this session of the roundtable. The committee will report back to parliament outlining the issues that were raised here today and will consider how those issues should be pursued. The secretariat is going to make sure that each and every one of you is kept informed of the outcome of these deliberations.

Proceedings suspended from 13:09 to 13:46

CLARKE, Dr Roger, Chair, Australian Privacy Foundation, and private capacity

CLOTHIER, Dr Reece, Private capacity

FALK, Ms Angelene, Assistant Commissioner, Office of the Australian Information Commissioner

HOLLAND, Mr Geoffry, Private capacity

KERR, Ms Deborah, General Manager, Policy, Australian Pork Ltd

McDONALD, Professor Barbara, Commissioner, Australian Law Reform Commission

PILGRIM, Mr Timothy, Privacy Commissioner, Office of the Australian Information Commissioner

CHAIR: Welcome to witnesses for this third session of the roundtable on drones and privacy. You need to note that these meetings are formal proceedings of the parliament. Everything said should be factual and honest, and it could be considered a serious matter if you attempt to mislead the committee. Our final session is primarily on the privacy issues relating to drone technology and to give this discussion some context and provide us with a starting point I will ask Mr Timothy Pilgrim, the Privacy Commissioner, to give us some brief opening remarks to set the scene.

Mr Pilgrim: When we are looking at technology such as UAVs we start from the position that, like most technologies, the technologies in themselves are probably considered to be neutral. Clearly, it probably goes without saying that it is the uses they are then put to that start to raise issues within the community. We can see with UAVs that there are potentially benefits for the community to gain from the use of UAVs, such as in search and rescue, and also for cost savings such as potentially doing survey work in remote areas. But, again, there are also some potential concerns that come out of UAVs. Those concerns come from the possibility for misuse of that technology by individuals or by other entities.

This is becoming more prevalent as we start to see that the technology itself is also becoming extraordinarily cheap. We have seen reports where you can buy UAVs at stores for under $400. These are fitted with cameras that can be run remotely from iPads or equivalent sorts of technologies. With such a new technology, the question comes down to how its use is going to be regulated. What are the ways in which it can be regulated so that we can still achieve the benefits that the technology can bring, at the same time as making sure that people have a right of recourse or a remedy if they believe their privacy has been invaded by misuse of those technologies?

I could do a quick overview of some of the laws, which you may have already touched on, that could come into play in various jurisdictions. Before that I would start by saying that contrary to a lot of views that you often hear around where privacy sits in the community, our community research, that we undertake every three to four years, consistently shows that the community remains concerned about what is happening with their personal information. The community is concerned to make sure that there are protections in place for that personal information. So rather than seeing it becoming an issue that is dying, as some commentators have said in the past, it is actually a constant within the community. Not only Australian research shows that but also international research backs that up. So if we had that starting point that there is an ongoing community concern around what is happening to their personal information and a concern that is heightened by new technologies which have shown new ways in which it can be collected in large amounts, we then need to look at the expectations around how it will be able to be regulated.

If we start to look at a high level of some of the laws that exist now, we can start with the federal Privacy Act, which is the one I am responsible for. The federal Privacy Act applies to most Australian government agencies at the federal level and many private sector organisations. It does set an overarching set of principles that those entities must comply with in how they collect, use, disclose, provide access to and secure personal information as part of their roles. But the Privacy Act itself does not actually cover the field.

By way of a quick example, within the federal Privacy Act there are a series of exemptions. Some of those exemptions broadly deal with an exemption for small businesses. Generally, a private sector business that has an annual turnover of $3 million or less is not necessarily going to be covered by the Privacy Act. That provides an area that may need to be looked at. There is also an exemption for media organisations in the Privacy Act. In the course of journalism, media organisations are not covered by the Privacy Act. Of course, the ACMA has a regulating role there under their codes and other provisions in terms of the media.

But coming back to the Privacy Act, it does not cover the activities of political organisations. That is not is necessarily one of the key focuses at the moment, but it has an exemption for political organisations as well. Importantly, it does not cover the activities of individuals in terms of their household affairs. Where that may come into play is if you, for example, have a neighbour who purchases one of the smaller drones or UAVs. If they

are undertaking that for purely their own interest, shall we say in terms of filming around their local neighbourhood, there would not necessarily be a right of recourse under the federal Privacy Act because of the exemption there for individuals. So there are some areas in the federal act that may be worthy of review or consideration.

If we then quickly look at the states and territories, there are a series of privacy laws within a number of the states and territories. These generally apply to the activities of state and territory government agencies as well, and tend to be limited to those entities. Also within the states and territories, as you probably have discussed at some point, there are a series of surveillance laws and possibly harassment and anti-stalking laws that may come into play as well.

I think the picture we are seeing there is that there are a number of laws that, in one form or another, do regulate the handling of personal information. First of all, what I do not think we do have—and I would be the first to admit this from my position—is a completely clear understanding of whether those laws as they currently exist are going to do the job, or whether, because of the patchwork nature of some of those laws, there are going to be gaps which need to be filled when we take into account how these new technologies can be used within the community. So I think one of the overarching questions that would be relevant to pursue through a discussion such as this is whether we think the laws are keeping pace with technologies like this and whether we think we have the right laws in place to deal with technology such as UAVs. I might leave it there at the moment because I know there is a time limitation.

CHAIR: I will pose a scenario to you that came up in the discussions earlier today and was in the press earlier this week regarding activist organisations that might be using this technology to fly onto private property and take footage or photographs of what is going on there. Are you aware, given your expertise in this field, if that activity would be in breach of any state privacy regulations?

Mr Pilgrim: Off the top of my head, I would hate to give a categorical answer because I am not that familiar with every aspect of each of the different surveillance laws, and whether or not trespass laws may come into play as well—that is questionable, but whether they do. A number of the surveillance laws may come into play in some of the states and territories, from my quick overview of a couple of them, but, I would suggest, possibly not consistent around the country in each of the jurisdictions.

CHAIR: Ms Falk, do you want to add anything to the statement that has been made by Mr Pilgrim?

Ms Falk: Perhaps I will just note some of the main principles that are inherent in the federal Privacy Act in terms of the requirements that are placed on those entities that are governed by the legislation. It is really a set of principles that focuses on transparency in the way in which personal information is collected. Partly that is about making sure that individuals have some notification about the collection of their personal information. There is a test of taking all reasonable steps to ensure certain matters are brought to people's attention. That is quite simple to achieve in some contexts, such as an online form or other such transactions. But in this kind of aerial transaction, the means of ensuring that kind of notification, so that individuals can exercise some control over whether their personal information is collected, perhaps become a little more challenging. You need to look at other methods for achieving that.

CHAIR: What happens when an individual who is notified of this sort of activity going on challenges it and does not want it to happen and does not want themselves or their property or any part of it to be in the exercise? Is there any provision for them to exercise that right?

Dr STONE: Does the fact that they are a corporation or a private farm come into it?

Mr Pilgrim: In terms of the federal Privacy Act we would have to look first of all at who is doing the filming. We do not need to dwell on it for too long, but if we are using an organisation which could claim the small business exemption within the Privacy Act as an example, the Privacy Act is not going to regulate what they are doing. They would have to look to some other law. In terms of the Privacy Act itself, if it was a corporation or a government agency that is covered by the act, and the person had concerns that it was being done in breach of the act, then they could deal with it immediately by seeking an injunction. There is an injunction power within the Privacy Act to try and have that prevented. But one of the concerns which I touched on around the overview of the laws—and which is the point I think you are getting to—is the ease of redress for individuals under any of these laws either to stop the practice happening immediately or to seek a remedy if they have suffered some harm or loss as a result. These are issues which aren't clear. But under the federal Privacy Act there would be an injunction power if it were against an entity that was covered.

Dr STONE: You mentioned, Mr Pilgrim, that an individual with, say, one of these little $400 devices is exempt from the Privacy Act in its use. But if they are using the device to go up to the 30th floor and look at their

neighbour in the shower, is that then overcome by a state law in relation to harassment or something like that? How does that work?

Mr Pilgrim: Again, without having full knowledge of each state and territory's various surveillance laws and the like, I would suggest that they would be better placed at the moment to use their privacy acts, if they do cover it, because clearly the activities of that individual—if it was just your neighbour in an adjoining apartment building—would not be covered by the federal Privacy Act. You would then have to look to what surveillance laws may do the job and whether they are actually framed in such a way currently that they pick up on technologies such as this and how they are used.

Dr STONE: In the scenario that the chair painted a minute ago, where he had the person, say, on a small farm and having someone who is perhaps in a vigilante group flying a device over the property to film some activity that they then want to use as evidence to prosecute a case of animal cruelty: is there any privacy law at the moment that could possibly be used with regard to the person trespassing over the property without permission with this piece of machinery? That comes into who owns the airspace, I suppose. And then there is the use of that material—the film, the pictures and so on. What happens there?

Mr Pilgrim: The Privacy Act deals with the collection of personal information, so you would have to look at the nature of the information that was being collected. Then you get into the context of what constitutes personal information: are you going to be able to identify an individual as a result of whatever the footage is that is being collected?

Dr STONE: Not the individual's property? It just has to be the individual person, a natural person?

Mr Pilgrim: It tends to be a natural person. However, if you then get down to—and this is probably going to a level of complexity you may not have time for—collecting any other information that is in the hands of the organisation that collected it, it could be used to identify an individual who may live on the property. So you get into an area there which becomes slightly grey.

But it is not just a matter of saying, 'I have a picture of your face, therefore I have collected your personal information.' There are other bits of information which people may not think is personal information in isolation, but if you are an organisation that then can join it up with other bits of information it could become personal information, so there is a grey area around there. That is why I think it is important to look at the raft of different bits of legislation we have to see whether they cover the area, particularly the surveillance laws.

CHAIR: Because you have to leave member for Murray, are there any other questions you would like to ask anyone?

Dr STONE: No, I will read the transcript carefully. But I think this is obviously a very grey area. We have state and federal gaps that we need to look at very carefully.

Ms CLAYDON: I was just thinking: there are all sorts of devices out there—not UAVs—that are currently collecting information—photographing people. Closed-circuit TV would be one example where I assume there must be some sort of law—I do not know how your privacy law intersects and cuts over there. Can you enlighten me? Or are they part of the exemptions?

Mr Pilgrim: It then goes back to how the Privacy Act sits. The Privacy Act itself, as Ms Falk was saying, is based around a set of privacy principles which are aimed to be technology-neutral in themselves; that is, that they can apply equally across traditional, some might say 'older-style' collection of information, such as paper copies, files, people writing into notebooks and storing personal information that way, through to storing information in computer data bases and also footage being collected such as CCTVs. The capacity is there for the Privacy Act to regulate the collection of personal information through a number of different 'mediums', to put it that way.

You then need to go back to looking at the entity that is doing the collecting. That is where it comes back to: what does the federal privacy act cover? As I said, it is government agencies and also much of the private sector. So, if a private sector organisation were using CCTV, they would need to give notice that it was being used and give enough information to people to know what is going to happen with that information should they want to find out and if they needed to access it; for example, to see whether it had information about them that was identifiable they would need to be provided with access. That is a common theme within the principles which sit across different types of technologies or different means of collecting personal information.

If you take it from the view that it is a technology-neutral approach, the issue then comes back to: who is the act actually covering? That would be more so, I would suggest, than the technology that is being used to collect it. So if an organisation, if I could take it one step further, is collecting information from your iPhone, for example, through an app, the same sorts of principles apply as long as the organisation that has provided you with the app is covered by the act. It is just that it has been collected through a different means of technology.

CHAIR: We might move on to the Australian Law Reform Commission. Professor McDonald would you like to give a brief comment on this topic for us?

Prof. McDonald: Yes. The term 'patchwork of laws' has been used often today and that is absolutely the case. I think it is made more complicated as well by the federal-state division of responsibilities and the history of different legislation. There are many ways of looking at the scenario you put up before. First of all, there is the common law of trespass. You start with that. It depends upon reasonable height and what is reasonable height in the circumstances. It is pretty untested other than the odd-commercial flight flying across. In addition to that there are exceptions in most state damage-by-aircraft acts, or civil liability acts as they are often now called, for the mere flight of an aircraft through the airspace at a height that is reasonable and in accordance with the air navigation regulations.

Those pieces of legislation were introduced in a very different time, in 1952, after a Rome convention which was aimed at protecting a fledgling commercial airline industry. So it was clearly protecting commercial flights from being sued for trespass through airspace. But of course it can now be relied on and it will be relied on as protection from liability for trespass in airspace. The million dollar question always comes down to, what is reasonable height in the circumstances and whether or not air navigation regulations are being complied with. But as we heard this morning from CASA the air navigation regulations are all about safety; they are not about privacy. So the fact that you have complied with regulations aimed at safety I think does not necessarily therefore make your activities lawful if in other respects the height is not reasonable in the circumstances. It is grey because it is untested and it will remain untested until someone takes action and the court gets the opportunity to determine it.

In addition to that of course, as Timothy has said, there are surveillance statutes around the country as you mentioned often this morning. They vary enormously as Mark Corcoran said before. They are a patchwork and that is one of the things we are looking at in our inquiry. In particular, as Mr Porter pointed out this morning, as well, the issue will be what is construed as a private activity that comes within the range of optical surveillance or listening devices. For example, South Australia, although it mentions optical surveillance devices, does not actually prohibit their use. So there is this variation around the country which is confusing I think to everybody.

As far the Australian Law Reform Commission goes, our terms of reference are to make recommendations in relation to serious invasions of privacy in the digital era. We have been doing that since 1 August last year and we are to give our final report by the end of June. We will be releasing our discussion paper in about two or three weeks with a number of proposals. One of our terms of reference is to design a statutory course of action—a civil course of action—for invasions of privacy, which a person could bring against another person for invading their privacy. A second term of reference asks us to look at other existing remedies, so we are looking at ways in which existing remedies and regimes could be strengthened to provide better protection and other innovative ways. Some of the things we are looking at and have had discussions with a lot of people are about regulatory gaps, about the surveillance statutes and so on.

I should mention one other point of liability for people using these devices. That is that under the state damage-by-aircraft acts or civil liability acts, if they actually cause damage on the surface there is a strict liability for any damage which is caused. For example, if they cause stock to get away and get damaged or if something falls out of the sky onto somebody or into a truck on a highway or something like that there are strict liabilities. Having listened to a lot of the discussion this morning, I am concerned about the lack of insurance that many of these people would have, because there is no requirement for insurance for these devices. I am told that while commercial operators will have insurance, and that will often be a condition on which they are given a job to do, there is no statutory requirement that insurance is carried for damage caused by aerial devices.

CHAIR: In the inquiry you are currently conducting, have you had a lot of feedback in relation to drone technology?

Prof. McDonald: It has certainly come up. We have had submissions from people who have been the subject of surveillance by drones. We have had submissions also from other organisations that know of the use or want to talk about the use of UAVs. Most of those are public submissions on our website, and there is quite a lot of information there. Some of those are confidential submissions, because of the nature of what has happened.

CHAIR: The ones that have been talking about surveillance, without going into too much detail, which parties have they involved doing the surveillance?

Prof. McDonald: There are two issues. The first point is—again, as we have heard today—there is an enormous amount of surveillance that is of very strong public interest use in terms of fire fighting, for example; and farming groups and so on can also see enormous benefits for themselves in using unmanned devices et cetera.

However, some farmers have been the subject of surveillance by different organisations and they feel that that has been an invasion of their privacy.

CHAIR: Mr Pilgrim, are you aware of your organisation having received complaints about drone technology and surveillance?

Mr Pilgrim: Not specific complaints from individuals, no. I would have to check whether we have had general enquiries on our enquiries line about it, but I am pretty safe in saying that I do not think we have had an individual complaint.

CHAIR: Would you be able to check that and let us know? That would be interesting.

Mr Pilgrim: Sure.

Ms CLAYDON: When is the discussion paper following your enquiry due?

Prof. McDonald: 19 March is the date we are looking at.

Ms CLAYDON: How will you distribute that? Are you seeking comment?

Prof. McDonald: It will be available on our website. We will be notifying people who have asked to be notified, and anyone we have had consultation with will generally be informed that it is out.

Ms CLAYDON: Then the final report is due in June 2014?

Prof. McDonald: In June, yes. So we have a very tight turnaround, I have to say, between the release of the discussion paper and the final report.

Ms CLAYDON: And you are reporting to whom, sorry?

Prof. McDonald: To the Attorney-General.

Ms CLAYDON: Thank you.

Mr PORTER: Professor, I look forward to reading the report; it will be fascinating, no doubt. Allowing for the divergence in state jurisdictions/laws pertaining to the Surveillance Devices Act, but accepting that they generally operate on the principle that it is prima facie unlawful to record or survey a person's private activity, however defined—and there are certain exceptions to that prima facie situation set out—as you have gone through gathering information for your report, those who advocate for a general tort of privacy, are they envisaging that that will sit alongside other privacy protection legislation such as the Surveillance Devices Act, or is it meant to cover the field?

Prof. McDonald: No, definitely, it will sit alongside. Because what it would be, if it were introduced, would be a civil cause of action that one person can bring against another individual or an organisation who or which has invaded that person's privacy.

Mr PORTER: Whether that be surveillance, trespass, data collection, or—

Prof. McDonald: Whichever. It might be by misuse of private information, which is a very typical basis for complaint, or it might be intrusion into seclusion, which is something that is probably broader than trespass, because trespass and nuisance has very strict title to sue requirements. You can only sue in trespass if you are the occupier et cetera. Same with nuisance; somebody can stand outside and keep you under surveillance—and not just visual surveillance—and not be subject to trespass because they are standing outside. So there are definitely some gaps in the common law. It is really intended to fill those gaps in the civil law of one person against another. But the Surveillance Devices Act provides for criminal offences, so it is quite different, and it is quite different from the whole regulatory framework, which is looked after by the IIC or ACMA.

Mr PORTER: I assume that would be the case.

Ms CLAYDON: Given your characterisation of the existing laws as being a bit of a patchwork at the moment, will your report be making recommendations as to whether there might be some value in seeking uniformity across state and territory laws, for example?

Prof. McDonald: Absolutely. In terms of the surveillance laws, that has been a very common response we have had from people—that uniformity across state boundaries is very highly valued. At the moment the lack of uniformity means that there is insufficient protection of people's privacy, because people do not know what is against the law and what is not. But it is also insufficient protection for organisations like those in the media, because they find it difficult to know what they are doing, and if they operate—as all media now do—across state boundaries, they can be breaking the law in one state and cross over a boundary and they are not breaking the law. So that clearly makes law much more complex. I think uniform legislation is high on everybody's list of wants.

CHAIR: I will move over to you, Dr Clarke. Would you care to offer the committee the Australian Privacy Foundation's view on this technology and the implications for privacy breaches?

Dr Clarke: I will jump to a couple of specific things, because a great many of the issues have been canvassed today at length. The first thing I would identify is that we do not talk about a single aspect of privacy, we talk about five dimensions. We find that is very important in order to draw out the different kinds of interests that individuals have in different contexts.

In particular, two are relevant here. We have done privacy/personal data nearly to death today, so that is one dimension well covered. But we identify privacy of personal behaviour differently. We identify that as the interest that people have in not being intruded upon by undue observation or interference with their activities, whether or not data is collected—after which it would then move into another space.

When we look at the Privacy Act—as Timothy has already provided in evidence—it is all but irrelevant to behavioural privacy protection. It was designed that way; it was designed to deal with data protection only. There was one small element that has been in it for some years in both sets of privacy principles—public and private sector—which was the requirement not to collect in an unreasonably intrusive manner, which was actually an action thing rather than a stored data issue. That was unusual internationally; it is in very few countries' laws, and unfortunately it is one of the many casualties of privacy protection features following the amendments that come into effect in about a fortnight's time. That clause is completely gone, so now the Privacy Act is almost totally irrelevant to the behavioural privacy side.

Mr PORTER: Was it used regularly?

Dr Clarke: I am not aware of it ever being used. It existed; it was an attractive idea. It gave a hook; it gave an opportunity to argue that privacy in Australia was more than just data privacy. But that particular element of that argument is now out the window.

With regard to the 30th-floor filming example that was used before, and the farm overflies which have arisen multiple times during discussions: the analyses that I have done—and here I switch from privacy foundation to my own hat, because I have done a lot of work in these areas as a researcher and consultant and I cannot speak for the privacy foundation's view on this particular aspect—are of a policy nature. I am not a lawyer. These have been that for a wide variety of reasons all of the available torts—harassment and stalking were mentioned in the 30th-floor filming example, trespass and nuisance in the case of farm overflies—are effectively irrelevant to all of the examples we are talking about.

You would have to go to very extreme arguments by lawyers before courts, expensively, in order to have any chance of bringing home any case based on any of those torts. For example, with the opportunity to use nuisance, when you have money—such as the film star who was set upon by paparazzi. If that were not used it was clearly because her lawyers advised her not to use it, because she used other elements of law in an attempt—as it turned out, fruitless—to get the paparazzi under control. So the conclusion I came to in that study is that none of those torts have any effect in this area of behavioural privacy.

Where data privacy is concerned, Timothy has said very nicely just about everything I had on this point except for one small thing, which is that the ACMA codes relate to media behaviour. Unfortunately the analyses, in this case the privacy foundation analyses, we have done have shown that the ACMA codes are a total waste of space when it comes to protecting individuals' privacy against media intrusions. So once again there is a huge gap that exists there.

Ticking on through the other sorts of things that could represent protections—and remember, we are looking for balance here—the privacy foundation is technology enthusiasts, lawyers and besuited people. We love some of the applications of drones. But looking for balance, we are missing it. Another area where we are missing it is in the listening devices acts in three states and with optical surveillance devices in the other five. From my reading of those laws as a non-lawyer and looking at it from a policy perspective, I have concluded that all of those cases are extremely limited in scope. For example, the term 'private to place' is defined in many of those statutes, and it is defined extraordinarily narrowly. In New South Wales it does actually include inside a car; but generally it is defined extremely narrowly, to the point where a great many of the examples that have been used, and that could be used, as test cases would not be subject to protection. They would not be offences. They couldn't be found.

One example has been the attempt in the recent ADFA cases. There were two of them, but in one particular case—the attempt to prosecute for the use of a surveillance device—the prosecutors evidently gave up. They eventually achieved a prosecution based on an extremely obscure section of the Crimes Act which has absolutely nothing to do with that kind of surveillance; it had to do with transmission of the image across a carriage service.

That was possibly the right outcome, but certainly a very strange way for it to be achieved. So that is indicative of the ineffectiveness.

I am not aware of a great many successful prosecutions under those various acts. Certainly under some of the upskirting and downblousing and similar legislation—which is related, but in many cases, different—there have been some prosecutions, but they are extremely specific instances, and they are not particularly relevant to drones.

The final point I wanted to make, drawing on the discussions over the last few hours, is that my reading of the Commonwealth Surveillance Devices Act is very different from the AFP's. The explicit answer was provided by the AFP that they cannot undertake surveillance without a warrant. I beg to differ based on a number of sections of the act. I just cannot see how those sections of the act—my papers explicitly state which sections of the act provide them with which powers under which circumstances. There are many circumstances in which they can conduct warrantless surveillance. Of course, that is a concern to all civil liberties organisations that there are inadequate controls in a lot of these contexts.

CHAIR: It may not have been the exact question, but I think the question was asked about their doing surveillance via drones over somebody's property, and they suggested that if they were doing that they thought they would need warrants.

Dr Clarke: There are at least three sections of the act that would give them the opportunity. One of them is extreme—they would have to declare public disorder. So one of them is pushing it. But the other two are far less extreme. Clearly he was answering a question verbally, and if he was answering in some particular, which I could not pick up from the context, then he might have been making a correct statement. But it did sound like a generic—

Mr PORTER: To be fair to the AFP, I think that question might have been mine and inelegantly put, and he was answering in very general terms.

CHAIR: We will follow that up and find out. If you could supply us with that work you have done, it would be good.

Dr Clarke: Yes, I have drawn it to attention; I have not provided copies, but the working papers are all on the web. I do not want to dwell too long on the law enforcement issue, because it is quite clear there are some extremely valuable applications in the law enforcement area, many of which would be strongly supportive of privacy, and many others of which, while invasive of privacy, would be well justified as a balance against privacy. So I do not want to jump in and attack law enforcement, but we have to be clear that there are many contexts in which controls are insufficient over existing surveillance.

One of the most general comments I want to make on the day is that the biggest problem is not drones per se; drones exacerbate existing massive deficiencies in surveillance law in Australia and, as an earlier presenter has said, we need to separate out those issues and solve the problems where the problems are. There will be some that are specifically drone-related, particularly in the public safety areas, and perhaps to some extent in the privacy areas as well.

CHAIR: Thank you, Dr Clarke, that was very good.

Ms CLAYDON: Earlier today we heard some evidence—I am not sure if her name is on this list, and I cannot remember her surname again—and it was suggested that their organisation had been working not only with industry but also civil libertarian groups. Have been privy to some of those discussions?

Dr Clarke: She did make that statement. She specifically used the words 'civil libertarian', which we do not quite use in Australia. The CLA has not had any contact from AAUS—Australian Association of Unmanned Systems?

Unidentified witness: No.

Dr Clarke: Neither has the APF. We are in fairly good contact with most of the other organisations in the area and we are not aware of those interactions. I was also very interested in the comments by Mr Mason to the effect that they had a code. I have searched for codes on both of their sites and I found nothing in the way of guidance and nothing in the way of obligations on members of either organisation. I have expressly searched all of the associations around the world as part of this research and I have not found those sorts of things. They were answering in present tense. It was not two months ago when I last looked at their website, but it would be helpful to see if they had some frame and if they had drawn it from somewhere. AUVSI, to the best of my knowledge, has absolutely nothing, because that is one of the many sites that I have looked at.

Dr Clothier: AUVSI does have a policy and code of practice which they floated last year for all of their members. AUVSI is the international association. It does not have a—

Ms CLAYDON: What is AUVSI?

Dr Clothier: It is the Association for Unmanned Vehicle Systems International. It is a US based association. It is very, very large. I could not tell you the number of members it has. But it did put up some privacy guidelines or principles, I think they called them, for the members. They were floated amongst its members, and I believe they are still there, to the best of my knowledge. That particular association does not have a presence in Australia.

Ms CLAYDON: Can I just ask a question generally of the Privacy Commission and the Australian Law Reform Commission. Have any of your parties been involved in discussions with industries about the production of any guidelines around the issue of privacy with UAVs?

Prof. McDonald: Not specifically with the UAVs. We did have discussions with the chamber of commerce, which brings up small business, and we have had discussions about the small business exemption generally and the lack of regulation of smaller organisations on privacy issues.

Mr Pilgrim: From the perspective of our office, no we have not had any discussions that I can recall with any organisations about codes. But I should add one thing which I could have pointed out as part of the overview of the laws. Under the federal Privacy Act there is a code-making provision that allows a code to be developed in regard to a specific technology, for example. So there is the power already there that I could approve a code to regulate the handling of personal information collected through technology such as UAVs. That can be done in three ways. It could be done by an organisation or an association coming to us to say, 'We want to lodge a code,' and we would assess it and approve it. I could identify a particular area, such as drones, and approach a group or a sector to say, 'Would you like to develop a code?' and in the absence of anyone taking up that offer I could develop the code myself through our office and then impose it on various entities. But, again, that would be restricted only to those entities covered by the Privacy Act.

Dr Clarke: From the viewpoint of civil society as a whole—I am involved in many other consumer organisations as well—we perceive a serious lack of consultation by a lot of the industries that are developing potentially intrusive technologies. Drones is one example, but media has been another one. We have been endeavouring for years to achieve meaningful discussions with the likes of the Press Council, with the likes of ACMA. We are unable to achieve it. We have tried with industry associations, of which there are several because of the diverse nature of the media. They basically rebuff civil society involvement.

What that means is that they lack insight into what the many different perspectives are of the many different segments. Civil liberties has a somewhat different perspective from privacy, a somewhat different perspective from various kinds of consumers. Of course there are people with particular kinds of disabilities who have different perspectives again. We do believe that that is a great weakness which is to the detriment of the effectiveness of the industry, because it means that problems explode later instead of having been addressed early on.

Dr Clothier: To some extent, with all due respect, I disagree with some of those—

Ms CLAYDON: Sorry, are you not with the Australian Privacy Foundation?

Dr Clothier: No.

Ms CLAYDON: Can you tell me who you are with?

Dr Clothier: I am with RMIT University, but I am also with the association that Peggy MacTavish was here earlier for. We have been very actively involved and, to possibly counter your argument, we have received no communique from you or your respective organisations, except from one in Victoria. That particular group—forgive me if I get the name incorrect, but I believe it is civil libertarians or libertarians Victoria, or something along that line—

Dr Clarke: Liberty Victoria.

Dr Clothier: They have been working very closely with us to address this issue, and I believe that I speak for everyone in the professional industry when I say that we treat it very seriously. That is why we are working very actively with that group to address their concerns. They, in conjunction with us, have been working to put up some recommendations. As Peggy MacTavish mentioned earlier, I believe those recommendations have been put to the Attorney-General. That is in response—agreeing with your comments earlier—to the fact that we believe there is not much protection for the rights of the individual in terms of privacy in this country at the moment and that there is a patchwork of legislation across this country that is very difficult to navigate from the perspective of industry.

We have not gotten as far as putting forward the code of practice that we do intend to generate for our members, but the last thing we would want to see as an industry is us being subject to a piece of regulation or

legislation independent of all of the other technologies and industries out there. If you look at what the Australian Law Reform Commission said in an earlier report about privacy law reform, they said it should be technology neutral. A lot of the themes of the discussion today have been technology neutral.

The surveillance devices acts at different state levels relating to audible or EO are all different. I can collect personal information with a lidar, and that will tell me exactly what you look like, or may I will use a radar another time. We need to step away from this idea that it is a specific piece of technology or a specific device and say, 'Let's protect the interests of privacy,' and ask, 'What does privacy mean? What is a privacy act?' Google Glass is a much more invasive technology that every person is going to be wearing in the next five years. So whether it is drones, Google Glass or the fact that I can collect metadata on your Facebook account and marry that up with your LinkedIn and actually track your movements, it is your personal information and it does not matter if it is your image.

The point I would like to stress to this forum is that it is an issue much broader than unmanned aircraft. Whilst the unmanned aircraft industry is very active in this space, we have served to be the call to arms, I guess, for broader privacy law reform, which in my mind, as a personal citizen of Australia, is needed irrespective of me with my unmanned aircraft industry hat on.

Ms CLAYDON: Given you have worked with Liberty Victoria and you have said you have landed on a set of agreed principles or recommendations, are you are able to articulate them? Do you have agreement on that?

Dr Clothier: I believe we can make those available, and we will. We were unaware of this forum when we were drafting those, and at that stage we did not have this in mind. But we most definitely will, and that is the intent. We want to get them out there; we want public comment.

Ms CLAYDON: That was not specific to UAV but a broader set of principles you are trying to work on?

Dr Clothier: Much broader.

Ms CLAYDON: That would be very helpful to provide.

Dr Clothier: Whilst the example of unmanned aircraft is being used, we have looked at this from a technology agnostic perspective because it is a much broader issue.

Ms CLAYDON: Indeed. So it would be very helpful to have some guidance as to where you and some privacy groups have found some common ground.

Dr Clothier: We will make that available. I will get in contact with them and make sure it is available.

Mr PORTER: Dr Clarke, I accept what you say about the fact that the essential deficiencies, as you perceive them to be, are not just related to unmanned vehicle technology. I presume that APF have some enthusiasm for a general tort of privacy. So I would like to focus a little bit on your views about the deficiencies inside the state and territorial jurisdictions' legislation on surveillance devices. What is it that APF conceives could be done better, or what changes would you like to see occur generally?

Dr Clarke: I am not prepared for that one in detail, but a couple of generalities are certainly feasible. One is that the definitions of 'private place' are extremely restricted, so it is not just a private place as an individual would perceive it to be. It is something that had been thrashed through in a legislature somewhere that is not terribly meaningful to most of us in the community. That is one problem.

The second is that the public place position in most of those statutes is that basically there is no protection—period. Individuals have private space within public places, and to deny that is to deny an awful lot about the normal functioning of humans. As an example, one of the best places to hold a private conversation is in a crowd, provided there is good noise and something that the crowd is focusing on, because the amount of white noise around you that is drowning out your conversation is huge. So there is considerable expectation—that is a dangerous word: expectation—and a considerable desire and need for private space in public places. That is not reflected in the laws. So those are a couple of the big ones that have philosophical difficulties with the existing laws.

Mr PORTER: The second of those would obviously potentially change the way in which CCTV is used at present.

Dr Clarke: Absolutely. CCTV is a major problem in this country because of the absolute lack of controls. Among the many policies that we have out there is a set of criteria for evaluation of CCTV systems, which applies as much to ANPR and to applications using drones. The eight principles there are by and large flouted by most of the applications of CCTV. Most of them are ineffectual. There are certainly some applications of CCTV which are a wonderful idea, properly resourced and properly placed. So the evaluations of technologies need to be undertaken much more carefully.

Dr Clothier: Following on from those comments, if we could view the use of, say, CCTV and move away from just unmanned aircraft for one second, it has to be a balanced appraisal of the benefits that CCTV offers the community. In your statement, CCTV was a problem. I know there is always a potential for misuse of technology, and there is always going to be a minute percentage of people or companies that we are going to be chasing. If we go back to CCTV, for example, is that outweighed by the 99.9997 per cent of good use that that technology brings to society? So now, if I look at it as a member of an unmanned aircraft industry, I would hate to see legislation put in place that hamstrings the many beneficial applications of this emerging aviation industry and its flow-on effects for mining, agriculture, surf-lifesaving—everything—through a piece of legislation that is chasing the 0.0003 per cent of people or organisations that will misuse it. That is just a comment.

Mr PORTER: One of the interesting potential applications of the technology is to replace fixed CCTV points. Potentially, it could be done to achieve the same effect in terms of law enforcement.

Dr Clothier: Yes, in terms of achievement, I do not think it really has much to do with the fact that the camera is flying; it is the same. You are capturing imaging or you are capturing personal information. You are going to hear this in all my comments: I think it needs to be technology agnostic. Whether it is on the end of a pole in a CCTV network or it is just going up and down the same street over and over again, whatever comes out of these discussions or whatever happens moving forward needs step away from the means in which it was collected or the vehicle upon which it was collected.

CHAIR: I think that is a theme that we have heard throughout the day. Even you, Dr Clarke, have made mention of that. Is that right? Is that the position that you are taking too?

Dr Clarke: Surveillance needs to be addressed in the generic. There are also some specific things in relation to drones—we are talking here about surveillance done by drones and surveillance activities using drones—because my analysis comes up with 10 points difference between static and drone based surveillance.

CHAIR: There is more capability.

Dr Clarke: There is a need for some technology specificity in regulation, but you have to start with a regulation agnostic base and then do any additional specifics you need. You have to do them carefully and you have to make them balanced. I totally agree with the balance point.

CHAIR: Unless there is another question, I am going to move on to Mr Holland, given you have the expertise in media and particularly media law and privacy. We heard from Mr Corcoran in an earlier session. There are always concerns regarding media intrusion into private individuals' lives, and I suppose there is a general concern that the technology we are discussing, drone technology, could push that even further. Could you offer some of your thoughts on that matter?

Mr Holland: I have recently met with representatives of a number of media organisations to talk about usage of drones. There is still amongst some media groups a reluctance to actually take the step of employing drones. There has recently been some discussion about the possibility of use of drones by the media over Manus Island. The media's concern in the development of privacy laws appears to be based on the need for a public interest exception or a public interest defence. I should also say there that I have also met with representatives from various animal welfare groups, and they are quite supportive of the development of privacy laws. I think media who for a long time have resisted the development of privacy laws have come to accept that it is going to happen in Australia, and now they are looking at how the laws can be developed in a way that ensures that the media's use of drones in a reasonable way—and it is the same with animal welfare groups—is protected, whether that be through a public interest exception or a public interest defence.

I agree with what has been said so far in relation to the need for a technology neutral approach in privacy laws, but I also agree with Roger that there are some specific issues arising from drones that need to be addressed, including the use of drones by organisations such as the media.

Ms CLAYDON: If there are any differences that you and Dr Clarke wish to point to in terms of static and mobile kinds of technologies, do you want to articulate what those areas might be, or is that too big a question?

Mr Holland: No, I think there are some aspects. For example, with static cameras notice is generally given. People are aware of it. If people do not want to be captured by CCTV they can change their route. That is not the case with drones. There is not the awareness of the presence of the surveillance device, and changing route will not necessarily facilitate escaping being captured by the camera. To me, that is one of the major differences in the way we are surveilled by static cameras and drones.

Dr Clarke: If I could just add a couple, supporting that one—surreptitiousness. One is extensiveness—the breadth of areas in which a person is subject to observation and the intensity with which it can be sustained, particularly when it reaches a point where somebody of interest is being followed. Both of those can change very

significantly when you move into a drone environment. They have to be designed to do that; it is a use question. It is not the technology that is evil.

Ms CLAYDON: Yes, it is the user.

Dr Clarke: So those are a couple of things that really lift the level. If I could just come back to that point about public interest justification, the APF totally agreed with everything you said, because their 2009 policy statement declared the importance of the public interest justifications, because privacy is dead without a free press—stone dead. So we regard that as very important, but we also articulated a set of eight headings with some clarification about what those eight headings were. That is what we sought to discuss with media organisations, and we have been unsuccessful. So if you guys can take them over and you can get in the doors, please do it, because the media really does need to have that as a balancing mechanism for both privacy and the broader public interests.

CHAIR: Mr Corcoran is shifting in his seat a bit! Did you want to respond, Dr Clothier?

Dr Clothier: In our analysis and our work looking at privacy law reform we did identify the issues with unmanned aircraft in terms of the actual exposure. I know a lot of the discussion has focused on the small multi-rotors today, because that is where a very large chunk—an estimated 70 per cent—of our industry will be. But, if we look just beyond that to the potential exposure of a single operator to fly one suburb, they could expose themselves to potential breaches of privacy for that whole suburb, of anyone who managed to even notice that they were being overflown.

There is the issue that a single operation can have a very high exposure, and then there is the practical issue. One of the operators mentioned doorknocking and going around. How do you go about disclosing the fact that you will be doing this activity? It may be that you are just looking at the power lines or the road condition, but you had to fly down the centre of the street and everyone on either side seemed to think that you were filming them as well.

These are the sorts of issues that we looked at, and the final one we picked up was about the practicality. If we did have a piece of legislation and some recourse for an individual who thought their private information had been collected, how would we go about enforcing it?

These sorts of things can be packed up and put in the back of a car without any evidence of who caught it. There are no markings on them. They are very small—I am talking about the smaller stuff here. What are the practical means of allowing that individual to follow up and get the redress that the law entitles them to, if this law existed? It is almost impossible. There is no policeman—CASA is not a policeman—to do this activity. We do not have the person on the street watching every plane and knowing where every one of them is.

CHAIR: I am going to move on from there and go on to you, Ms Kerr. I suppose it has been a recurring topic of the day—it has featured in the news recently—about animal rights groups sending in drones to farms to look for what they think might be unlawful or unethical activities taking place. I think you might be here to talk about that in particular, but I will let you talk on behalf of your membership in Australian Pork Ltd.

Ms Kerr: Thank you for the opportunity to speak to the roundtable. Certainly a lot of the issues raised in this session are similar to the issues that I was going to raise: the fact that there is a myriad of legislation across states and not all of it is consistent, and the issues around privacy and invasions of what farmers see as their privacy not just by drones but by all surveillance devices. For us the issue is not drones per se; the issue is misuse of technology for other purposes, so it is a wider issue than just drones.

I think it is fair to say—Dr Clarke was correct—that the opportunities for farmers to undertake some sort of litigation against perpetrators that have entered their property either on foot or in the airspace are quite limited. They have to be able to identify the perpetrator to be able to take action; that is a rarity. They have to be able to demonstrate that they have had damage, and the courts to date have not accepted that farmers have been damaged very much at all. There are two pieces of case law. Nobody has talked about case law yet, but there are cases called the Lenah case and the Windridge case; the latter involved a piggery in New South Wales. The ability for those farmers to take any sort of action has been quite limited.

One of the issues relating to this inquiry that have arisen is around what is deemed to be private on farms. For example, the activities of production sheds in piggeries, poultry production sheds and lot feeding of poultry and livestock, including beef cattle, are not deemed to be private at all. So the ability for farmers to take action is limited by the fact that their production facilities are not deemed to be private. That limits the ability for farmers to take any sort of action to redress the invasion of their property. The potential issue for a lot of livestock farmers, including our own piggeries, is biosecurity. If you have somebody walking onto your place, it poses an

immense biosecurity and disease risk for our producers and our pigs which creates its own animal welfare issues, the very things that some of the activist groups are seeking to address in using this sort of technology.

The other important point to note for us is the misuse of the images or videos that are taken. It could be months down the track before those things are made public, and often the images are uploaded onto internet sites or video sites that are not Australian based. There is no ability for us to have those images taken down. It is very difficult for farmers to have that issue addressed. There is a whole range of privacy issues that basically limit the ability of farmers to take any further action to address some of that misuse.

CHAIR: What do you want to see to remedy that situation?

Ms Kerr: I think there is a range of things. The issues around defining what is private property and what is not needs to be dealt with, and I think Dr Clarke has made some comments about that. For us, with production facilities and farm facilities, farmers deem them as private. It is freehold land, largely, and they would deem that that is an invasion of privacy. In fact, many of them would feel similar to what homeowners feel if they had been burgled: they would feel that they had been traumatised and that they had been invaded; they would feel dirty and that their staff had been put at risk. So dealing with the issue of privacy is a high priority. Some consistent approach to surveillance device legislation across all of the jurisdictions would also help deal with some of these issues. I think, at the top of my mind, some consistent approaches to regulation is needed. But, for us, there is also the issue of the existing case law. Any changes to regulation must be able to deal with the existing case law that is out there.

Ms CLAYDON: I do not know if you have this information, but what would be the ratio of your membership that is privately owned as opposed to corporate farming.

Ms Kerr: I would have to take that on notice. The number of producers would be quite a small percentage, but the amount of production is at the high end.

Ms CLAYDON: Sorry, what is there difference there? The number of producers versus—

Ms Kerr: The actual production. Of the number of pigs or sows, for example, a lot is corporate owned. But there is a large number of producers who have small numbers of pigs. If you are talking, say, less than 500 pigs, there is quite a significant number. As to which ones are operating under corporates, there could be family farms up to corporate structures as well.

Ms CLAYDON: You mentioned your concern about possible biosecurity breaches. Have there been any to date?

Ms Kerr: The issue is whether they are actually taking going onto properties consecutively. If those that are coming onto a property are going to two or three in the same night or within three days, that increases significantly the biosecurity risk. Have there been disease outbreaks as a result that? Not to my knowledge. But the fact is we take biosecurity incredibly importantly on pig farms. We record people coming onto the property and we make people change protective equipment between sheds—all of those things are in place on a property to maintain biosecurity on the farm and within sheds on the one property and between properties.

Ms CLAYDON: Finally, this is a question that I put to the Voiceless when they were here. Given that the availability of free-range pork on the market is limited and there is some level of consumer interest in that area, I could see that there would be some pork producers that could see the value of some kind of technology like this—perhaps being able to verify the free-range practices and therefore have a commercial plus to their produce as well. Is anybody using it at the moment for that kind of purpose?

Ms Kerr: No, but we have our own quality assurance program called APIQ. It incorporates our free-range and outdoor-bred certification programs that are based on hazard principles. In terms of verifying those credentials, we do that anyway. That is audited by third parties, so we do not need drones to be able to do that.

Mr Holland: This is one area, though, where the use of drones for animal welfare organisations has been effective. A number of prosecutions of farms where there has either been mistreatment of animals or prosecutions under the Australian Consumer Law, the Trade Practices Act, has arisen because of information obtained either through static cameras that have been installed or, more recently, through the use of drones, particularly in the areas with the ACCC taking action for farmers or producers of both meat and eggs that are claiming that they were free range, or raised under certain conditions, and yet the surveillance showed that that was false.

So there has been a use as far as consumer protection goes for drone footage. It is certainly a complicated area and I think the privacy interests of farms have to be taken into consideration, but, as has been pointed out, a large number of them are corporations and that raises the question of whether privacy is going to be seen as a basic human right that attaches to the notion of human dignity and should not extend to corporations as was discussed

in the Lenah Game Meats case where the court was of the view that certainly privacy rights did not attach to corporations.

Ms Kerr: If I could respond to that, I think our view would be that it is not the role of activist organisations to actually undertake those activities. We would prefer to see the appropriate regulators who are accorded the relevant authority to investigate those matters actually able to undertake those activities. We certainly would not be supporting activists to be undertaking drone activities above our producers' properties.

Prof. McDonald: Sometimes this corporate issue tends to sideline things, because often the activity might actually be an invasion of the individual's privacy who might be members of the corporation, just as it is in defamation. Corporations cannot sue for defamation now in this country, but the individuals might be defamed. Similarly, if there is a statutory cause of action, individuals might still have their privacy invaded even though there is a corporate entity owning the actual property, which would stop those individuals suing for trespass, because they are not the occupiers, but it would not stop them suing for invasion of privacy.

Mr Holland: Certainly, yes.

Dr Clarke: If I could just toss in the Privacy Foundation perspective on that one, we attend to distinguish economic enterprises from social person(s) involved. So family and employees on these farms, whether they are owned by a corporation or whether they are owned by a partnership—the ownership to us is an irrelevant question—the interests of those individuals… Well, there is no public interest in disclosure of the information about those individuals, because they are operating in a social capacity. But there is no privacy protection for the economic aspects. There may be protections of other kinds, but that is just not a matter that privacy interests are particularly concerned about. So we come at it from another perspective—not the corporate versus unincorporated but rather the individual/social versus the economic.

CHAIR: Do you think it is right that the economic interest is not afforded some sort of privacy—

Dr Clarke: Not privacy; privacy is an explicitly human right and there are squillions of things to support that. There is an interest, and I do certainly would not dispute and APF would never dispute that there is an interest of an economic kind on the pork farmers side—be it small, medium or large—as well as other kind of interests of a regulatory nature and an animal wellbeing nature. There are many of these things to be balanced, so it becomes an exercise in balancing. The idea that you would either completely ban and criminalise and impose capital punishment for somebody who flew a drone over a farmer's property is as silly as the other extreme. There has got to be some sensible outcomes found.

CHAIR: I know it is a bit of a philosophical point but, obviously, you can have a family that own a farm that has set up a company structure to carry on that enterprise. It is their enterprise, it is a human endeavour—their work, their toil. Surely it is a human right to protect what someone has essentially created, and having an invasion into their property—the property which they are actually making a living out of—is an invasion of privacy.

Dr Clarke: We distinguish between the privacy of the individual in the social sense and the other kinds of interests that they have in an economic sense. For instance, I work from home. I have just got to face up to the fact that a variety of organisations would have an interest in what goes on in my office and far less interest in what goes on even in the hallway, let alone in the rest of the house. So we tend to distinguish it that way. I am not suggesting it is easy to distinguish, because some of the economic activities may occur on the front veranda of the house, so it is not an easy principle to carry through and operationalise, but that is the approach that we would take to it.

Mr PORTER: I find that a very interesting way to try to create a distinction. If you are a person employed in an enterprise—whether in an office, on a farm or by a corporation—and engaging in activities which you are paid to do and which in that sense may be described as economic activities, I fail to see how those are not a matter of some privacy, because they are human activities which would otherwise not be surveyed.

Dr Clarke: Sitting at a desk doing things of a private nature—phoning the wife to organise who is picking up the kids tonight and what is being picked up at the shop on the way home—are private activities undertaken in a workplace environment. Yes, we would certainly argue that those things are subject to privacy protections because they are private matters and not economic activities.

Mr PORTER: But that would mean that, theoretically, the APF would accept that there could be surveillance by employers of employees during the course of their employment.

Dr Clarke: Our policy is quite explicit. Yes, there are certainly circumstances, subject to appropriate justification controls and all the rest of it, where surveillance of individual employees in the workplace is entirely justified. It is the constraints on that and the existence of private space even within that workplace environment that we argue for.

Ms CLAYDON: I just want to clarify something with Ms Kerr. I think I have it correct that one of the issues you raised was that there could be privately-owned farms with the production facilities on those farms not deemed to be private.

Ms Kerr: Yes. For the purposes of the surveillance legislation and so on, the home on the farm is considered private and would be accorded privacy legislation. But the production facilities—in our industry's case, the sheds where the pigs are produced and where sows go through their pregnancy and deliver their litter—are not deemed to be private. So I am not accorded privacy.

Ms CLAYDON: Under what laws? What are you referring to there?

Ms Kerr: It is case law.

Ms CLAYDON: Thank you.

CHAIR: I am going to get you, Mr Pilgrim, to wrap up with a question that I am going to pose. Do you think, after the hearings today, that there is a need for greater privacy regulation when it comes to this technology or a need for perhaps just pulling in all of the different patchwork that we have over the nation and having it clear in the one area?

Mr Pilgrim: That is a big question which my colleagues at the Australian Law Reform Commission looked at for quite a number of years some years ago in terms of the nature of privacy law in Australia. I think that there is a patchwork and that there is not sufficient clarity within the community. I would suggest that there is a lack of clarity even within those of us who work within the field around whether the laws are currently sufficient to deal with situations such as emerging technologies. I take the point very clearly, and we try to subscribe to the fact that we are talking generally about emerging technologies—of which UAVs are one. So I think there is a role for someone to take the lead in working out whether in fact the current laws are sufficient to protect the community's privacy rights in the area of emerging technologies.

I should have added at the beginning that I wrote to the former attorneys-general on this issue and that, when Mr Dreyfus was Attorney-General, he had taken the step of writing to all his colleagues in the states and territories to assess their surveillance laws and the like to see whether they were meeting the needs of this particular technology. So I think there is still an outstanding question about whether the raft of laws we have within the country at state and Commonwealth level are sufficient to look at and deal with emerging technologies that can be used for surveillance purposes.

CHAIR: I am quite well aware, Professor McDonald, that this is the work that you and your agency are doing. We look forward to seeing that.

Prof. McDonald: Yes, we are certainly doing as much as we can in the time that is allotted to us to do it.

CHAIR: That ends the roundtable. Thank you very much for participating in it. As a committee we are going to report back to parliament outlining the issues that have been discussed here today, and we will consider how those issues should be pursued. The secretariat is going to make sure that you are kept informed of when we report back. Thank you very much, each and every one of you, for your attendance and participation in this today. I also thank very much Thomas and the secretariat staff for their time in pulling this all together.

Resolved that these proceedings be published.

Committee adjourned at 15:05