Commercial RPAS and Privacy

ACUO submission to the Australian House of Representatives Standing Committee on Social Policy & Legal Affairs

28 February 2014

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

About ACUO

* The Association of Australian Certified UAV Operators Inc. (ACUO) is a not-for-profit association first started in 2009 by seven of the then eight CASA certified UAV operators. ACUO was formally registered as a legal entity in the State of Queensland on the 31st March 2010.
* The ACUO membership has decades of experience in commercial UAV/RPAS operations and an impeccable record of safety. Since commercial UAV/UAS/RPAS operations formally began in this country in November 2002, there has not been a single accident or incident specifically resulting from ACUO member's thousands of hours of commercial UAV flight operations.
* This record of achievement by ACUO members is a major source of pride, and is a status we are eager to protect by maintaining the highest standards of safety and risk management.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Terminology

* The terms ‘Unmanned Aerial Vehicle’ (UAV); ‘Unmanned Aircraft System’ (UAS); ‘Remotely Piloted Aircraft System’ (RPAS); and ‘Drone’; essentially all mean one and the same thing, that is:
  - “An aircraft [or aircraft-system] that is flown from a remote location without a pilot located in the aircraft itself.”

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Terminology (Cont.)

* Normally the pilot associated with the system is located on the ground, but the remote location in question can equally be aboard a vehicle, a boat or even a manned aircraft.

  - ‘UAV’ was the original term adopted by CASA in July 2002 and is still widely in use including much of CASA certification, licencing and guidance material.
  - ‘UAS’ is the more up-to-date internationally accepted term in use today, including with CASA.
  - ‘RPAS’ is the new ICAO adopted terminology - soon to be adopted internationally, including CASA
  - ‘Drone’ is a generic term used by the media, predominantly in relation to military systems but more commonly these days referring to all ‘Unmanned’ or ‘Remotely Piloted’ aircraft. Historically, and today, a military drone is an unmanned aircraft used for training air defence weapons operators.
  - Recreational ‘remotely piloted’ aircraft are termed ”Model Aircraft”, and are flown only for sport and recreation purposes, under the administration of the MAAA and the Civil Aviation Safety Regulations (CASR) 1998 - Part 101.G.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

The nature of an evolving problem

PART ONE

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

What is the issue?

* Fear of RPAS being used to monitor private citizens.
* Fears of invasion of one's "private life" – stigma of diminished social worth.
* Fears of the removal of one's freedom to go about one's day to day activities without interruption or interference by actors whom we consciously choose not to play a direct role in our personal life.
  - Various scenarios but police powers are a major focal point for activists, particularly in the US but increasingly in Australia.
* Fears of an absence of appropriate legal protections to ensure our underlying civil and human rights are upheld.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Why this issue?
Why now?

* The long war is ending and RPAS are coming home, including the return of ADF systems to Australia.
* Privacy was an issue at the start of the long war
  - E.g. US Patriot Act.
* Privacy has been put back on the table as a political issue by Google / Google Streetview/ Facebook / mobile devices.
* For all sides of politics privacy is an acknowledged human right. ACUO acknowledges privacy as a human right.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Defence RPAS and individual privacy

* By and large military RPAS are not the direct issue.
* Armed forces in Western-style democracies are constitutionally and legally regulated to prevent their use against their own citizens.
* Most Western-style democracies do allow use of military capability to aid and assist civilians during times of national emergency (e.g. floods / fires / earthquake).

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Armed Reapers over my backyard?

* Public perception of military RPAS is heavily focussed on ‘drone strikes’ – i.e. weapons capable systems.
* This linkage distorts legitimate debate on privacy matters.
* The distortion comes from all sides of politics.
* The distortion is often intentional and because of this, gets the most attention.
* US has emerged as the hotbed of this aspect of the debate
  - The US congress moved in late 2012 to short circuit this:

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

US FY2013 Defence budget bill H.R.4310

* **SEC. 1084. PROHIBITION ON USE OF INFORMATION AGAINST A UNITED STATES CITIZEN GATHERED BY UNMANNED AERIAL VEHICLE WITHOUT A WARRANT.**

"Notwithstanding any other provision of law, information acquired by an unmanned aerial vehicle operated by the Department of Defense may not be admitted in a Federal court, State court, or court of a political subdivision of a State as evidence against a United States citizen unless such information was obtained by such unmanned aerial vehicle pursuant to a court order."

* Approved by US House of Representatives 18 May 2012.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

The civil picture

* We accept that a change is coming… and with it great opportunity.
* Development of the commercial market will see RPAS become increasingly commonplace in our societies.
  - Potential govt. users: law enforcement, emergency responders, environmental compliance.
  - Potential commercial users: surveyors / assessors / aerial filming / media.
* It is critical to understand that in the civil market it is not the RPAS that is the core of the business, it is the data the RPAS generates.
* What data contains is at the heart of the privacy debate.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Worrying scenarios 1

* Ms Jones is showering with her lover in an upstairs bathroom.
* The operator of a commercial VTOL RPAS filming a real estate video to assist the sale of neighbouring house gains an inadvertent glimpse of what is happening.
* The operator then elects to intentionally film Ms Jones.
* The commercial RPAS operator thinks the footage of Mrs Jones is ‘hot’ and emails it to a friend.
* The friend posts the video onto You Tube.
* The footage goes viral within hours and is seen by many within her community and her workplace…

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Worrying scenarios 2

* A major industrialist plans to quietly marry his actress girlfriend at a mountain retreat. The guest list is intentionally limited and the location kept quiet.
* A media organisation hires a commercial RPAS to track a known guest as he travels to the event, and then films the outdoor wedding with a high definition camera.
* The media organisation broadcasts the footage live and the location of the wedding is revealed, leading to a paparazzi invasion of the wedding feast…

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Worrying scenarios 3

* A young man uncertain of his sexuality has an encounter with another male in a park.
* The encounter occurs as a commercial RPAS operator, contracted to monitor night time movement of feral animals in urban areas, passes over the same area.
* The young man becomes aware of the RPAS and flees.
* Alone in his apartment and already confused about the encounter in the park, the young man becomes convinced he has been filmed by the RPAS. Fearing the imagery will become public he takes a drug overdose… His suicide note makes specific reference to the presence of the RPAS.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

An inherent tech problem or…?

* RPAS are privacy neutral as a technology.
* The key issue is what is done with the data the RPA collects - That is, data regarding any individual whose identity is apparent or can be reasonable ascertained.
* In the military environment RPAS-generated data is part of a very well structured command and control chain with security restrictions an inherent feature.
* In the civil domain the data command and control, and security structures for RPAS data, are less clear.
    - Variations inherent by virtue of whose RPAS is involved...

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

A human problem

- Regardless of the scenario it is how humans use the data that an RPAS provides, that constitutes the basis of any potential privacy breach.
- Because we are talking about humans we need to understand that we are dealing not just with the possibility of actual privacy breaches, but also *fears* of privacy breaches.
- We cannot legislate or regulate to remove fears, but we can diminish the impact they have by adopting appropriate structures that provide inherent protections and means of recourse for individuals.
  - This is critical to our "social licence" as an industry.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Recognition of privacy in international law

* United Nations International Covenant on Civil and Political Rights (1976) – Article 17

  "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation."

* Further:

  "Everyone has the right to the protection of the law against such interference or attacks".

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

What is sensitive?

* Information or opinion about an individual's:
  I. racial or ethnic origin; or
  II. political opinion; or
  III. membership of a political association; or
  IV. religious beliefs or affiliations; or
  V. philosophical beliefs; or
  VI. membership of a professional or trade association; or
  VII. membership of a trade union; or
  VIII. sexual preference or practice; or
  IX. criminal record;
* In the RPAS specific context we need to relate this to information about an individual's *state* and their *actions* in the context of *location*.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Where is privacy?

* Location is a critical element of the RPAS privacy challenge:
  - Ms Jones can reasonably expect that her actions in her bedroom will not be subject to public viewing unless she chooses.
  - The industrialist marrying an actress may have sought privacy but hosting the event outdoors inherently alters that expectation.
  - For the young man in the park the expectation of privacy is significantly diminished despite the use of darkness to reduce potential disclosure of his actions.
* The *where of privacy* will be an ongoing issue as the civil RPAS market develops and will form not only the basis for lawsuits for alleged breaches but also be the foundation of most defence cases.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

A notional privacy architecture for RPAS

Part Two

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

A notional framework – 'Privacy LITE'

* A multi-layered approach based on extant constitutional, legal, regulatory and corporate governance structures
  - i.e. Work within existing legal framework rather than wait for laws and regulations to change.
* Overarching objective is to ensure airspace safety mission is not jeopardised by attaching new obligations onto regulators.
* Secondary objective is to keep the framework as simple as possible and as consistent as possible with existing legal structures regardless of RPAS operating countries.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Capstone layer

* Existing national laws:
  - Constitutional.
  - Human rights.
  - National security.
  - Data protection.
* These provide a generic ‘big picture’ / ‘big policy’ framework on a country by country basis that sets out addressable privacy law requirements - albeit to varying degrees but sufficient to provide a starting point.
  - i.e. We work to comply with what the baseline of our laws already require and allow. We work to evolve laws as required.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Capstone examples: USA

* Constitutional protection of privacy via amendments:
  - 4th Amendment – protection against unreasonable search.
  - 9th Amendment - protection of rights not specifically enumerated in the Constitution.
  - ie privacy protection an implicit structure with deeper interpretation developed by case law.
  - 4th Amendment case law already forms the basis of legal right of US police forces to conduct aerial search using manned aircraft.
  - 4th Amendment also most likely basis for future privacy challenges to RPAS operations.
* Federal Privacy Act of 1974 – controls collection, maintenance, use and dissemination of personal data held by Federal departments and agencies.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Capstone examples: Australia

* No inherent constitutional protection of privacy.
* No national bill of rights but ICCPR 1976 has legal recognition an annex to the Human Rights Commission Act of 1986.
* Federal Privacy Act 2008 (as amended).
  - Treats imagery as data, but assumes data consists of words. Needs some adaption to reflect changing technology as a result.
  - But requires privacy to be assessed by all Federal Govt. Departments and agencies, and large companies as an aspect of corporate governance.
  - Key compliance mechanism is the conduct of Privacy Impact Assessments (PIA's) – Federal Privacy Commissioner already signalling commercial UAS operators may need to use PIA's.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Second layer: Airspace regulators

* Privacy activist community is pushing, particularly in the US, for airspace / air safety regulators to take on privacy oversight and compliance issues.
* But, this threatens to distort the primary function of such regulators – which is to ensure safety above all else.
* Our position should be to "leave unto the airspace regulators what belongs to airspace regulators".
* But regulators can help the RPAS industry in practical ways….

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Regulator's privacy obligations assumes passengers….

* As a general principle most airspace regulators have a privacy obligation with respect to the handling of aircraft *passenger* data – A combination of national privacy / security / data handling laws.
* But the issue of how regulators should handle what is done with data collected as a result of aircraft operations is new territory - though there are some precedents:

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

But the FAA has at least one obligation

* US Title 49 (Transportation), Section 40128: Over flight of national parks-
  - "An air tour management plan for a national park … may establish conditions for the conduct of commercial air tour operations over a national park, including commercial air tour routes, maximum or minimum altitudes, time-of-day restrictions, restrictions for particular events, maximum number of flights per unit of time, *intrusions on privacy on tribal lands*, and mitigation of noise, visual, or other impacts."
* Means FAA has to look at privacy impacts on the ground in a specific circumstance.
* Originally interpreted to mean restrictions on direct over flight, but RPAS can perform stand-off surveillance...

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Safety is an enabler for privacy

* Regulators most effective contribution to privacy debate will be to ensure clear rules for how RPAS fly in national airspace in the first instance.
* Licencing, certification, flight ceilings, operating restrictions etc. already mean that commercial RPAS operators cannot simply fly out and randomly select a private citizen to track, monitor and otherwise ruin their day, regardless of circumstance.
* i.e. the underlying mission of regulators to ensure safety, provides an indirect contribution to the protection of individual privacy in a wide range of circumstances.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

US 4th amendment plus FAA regulations…

* The combination of constitutional protections and airspace regulations already combine in US case law to provide the basis for use of manned aircraft in law enforcement operations in the US:
  - California V. Ciraolo - 1986 - Anyone who flies can see into a backyard therefore there is no privacy in that space against police surveillance.
  - Dow Chemical Co. V United States - 1986 - Aerial photography of commercial facility can be conducted by a Govt agency without a warrant as long as flying "lawfully within navigable airspace".
* Broad thrust of current US case law is that conduct of an act in any outdoors area cannot be construed as private.
* But that case law also strongly points to the assessment that in the US, law enforcement RPAS operations below 500ft AGL will require a warrant unless specifically authorised by local ordnances.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

The Australian specific context

* Existing CASA regulations prevent RPAS flying anywhere, anytime.
* There is a large cadre of CASA certified RPAS operators, 70 and counting.
* The safety record of those 70 certified operators is outstanding.
* BUT, Australia has a huge problem with uncertified operators.
  - E.g. The Sydney harbour bridge incident, and the question remains as to why the owner / operator of that system was not prosecuted for clear breaches of Australian regulations.
* ACUO holds that the largest single prospective source of privacy breaches involving RPAS will directly involve illegal and uncertified operators.
  - If basic flight regulations are not going to be enforced by CASA, what hope is there for enactment of any RPAS privacy regime?

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Third layer: Local and state ordnances

* In most western democracies there already exists a wide range of state and local government ordnances which act to protect us against unwarranted breaches to our liberty.
* We most often look to this level of government for recourse where we have direct experience of crime.
  - Mrs Jones in her shower could well be protected by statutes originally intended to deal with neighbourhood prowlers or controlling the public area activities of commercial photographers.
* Push is underway in the US for model ordnance to assist local government in shaping appropriate laws for RPAS.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Australian state laws

* No Australian state or territory save Queensland has enacted any form of legislative control over RPAS operations.
* The Queensland legislation is specific to the G20 and bans all forms of RPAS and model aircraft operations during that event.
  - There was no consultation between the QLD Government and the Australian RPAS community before that legislation was enacted and the precedent is unsettling.
* The Federal Attorney General last year asked all States and Territories to review their jurisdictional laws with respect to RPAS operations.
  - We are encouraged by this step but again, there has been no engagement with the RPAS operators community.
  - A clear outcome for this review needs to be national harmonisation of applicable state laws – aviation is by definition cross-border.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Fourth layer: Industry itself

* The RPAS industry is directly bound by the architecture of national, state and local laws which act to protect privacy.
* Where exceptions to those laws exist (e.g. small business exemptions on the basis of regulatory burden) there remains the potential for legal action in the event of breaches.
* As an industry we accept legal structures bind us across a variety of domains and we develop appropriate policies and governance structures to ensure we comply.
* Privacy is no different to any other regulatory issue:
  - we need to accept its challenges and act accordingly.
  - Our alternative is to accept the lawsuits that will come and live with the consequences.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

A model governance framework

* The corporate governance structures required for privacy will have close parallels to the measures we take for risk mitigation – indeed they can be treated as an element of the same.
* The challenge is how to approach this. What are the models? What are the precedents?
* One conceptual approach may be to adopt the concept of the privacy impact assessment (PIA) developed by the office of the Australian privacy commissioner.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

The Australian PIA model

* What is a PIA? "An assessment tool that 'tells the story" of a project from a privacy perspective".
* A PIA:
  - Describes how personal information flows in a project.
  - Analyses the possible privacy impacts on individuals' privacy.
  - Identifies and recommends options for managing, minimising or eradicating these impacts.
  - Analyses the project's effect on individual privacy.
  - Helps find potential solutions and manage privacy impact through this analysis.
  - Can make a significant difference to the project's privacy impact and still achieve or enhance the project's goals.
  - Encourages good privacy practice and underpins good public policy in the project or, in the private sector, underpins good risk management.

Source: Office of the Australian Privacy Commissioner 2010

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

What would an RPAS PIA encompass?

* Some initial thoughts:
  - A PIA would seek to provide a detailed description of RPAS operations at a generic as well as in notional mission specific contexts
  - A PIA would cross reference standard operational practices against the potential for privacy breaches at all stages of an RPAS mission - the starting point for this would be our standing operational concepts documents and extend to our data storage and distribution practices.
  - In turn a PIA would provide the baseline for introduction of guidance on handling privacy issues into our operations manuals and operate training requirements.
  - A PIA would provide the first line of corporate defence against lawsuits when and where they arise.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

PIA in an operational context

* All RPAS flight operations are constrained by existing law to specific flight zones. There is no legal capacity to fly anywhere at will.
* Flight zones are scoped geographically and are highly localised. Standard RPAS operational procedures utilise 'geo-fencing' to maintain compliance with the approved flight zone.
* Direct fly overs of populated centres / facilities is not legal.
* Flight operations within that flight zone must be planned. The PIA process would aim to facilitate identification of potential privacy risks within that planning stage.
    - E.g. Identification of sensor boundaries relative to geo-fences.
    - E.g. Identification of likely centres of human activity relative to approved flight zones and proposed flight path. Sensor alignment planning to avoid "over-reach" by sensor.
    - E.g. Use of motion detection software in optical sensors to alert operators to presence of human activity necessitating requirement for imagery screening to ensure no breach has occurred.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

New technologies of assistance

* Automasking is already available as a standard element of commercially available imagery processing software – Google for example, already fields such systems as part of its Streetview architecture.
* New generation automask software capabilities are emerging which require no human intervention and automatically blur human facial characteristics as the imagery is collected.
* Automasking, in conjunction with the use of the PIA model, will greatly assist in reducing the possibility of privacy breaches.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

How do we move forward?

* The privacy debate cannot and will not be simplified out of existence – it will remain a complex challenge.
* However this is not a challenge on the scale of RPAS airspace integration.
* The RPAS community needs to anticipate strong national debate at a national level as the challenge is played out.
* But the starting point is to recognise there are legal structures already in place which address many of the challenges now being identified.
  - There are ways forward and conceptual solutions accessible.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Final thoughts…

* The privacy challenge is an opportunity.
* There is an obligation on the global RPAS industry to show it consists of good corporate citizens whose interests are identical to the general community.
* The global RPAS industry must act to ensure that its corporate governance structures are such that its ‘social licence’ to conduct commercial operations is not diminished as a result of this debate.
* Regulators and governments must recognise that all sunrise industries carry with them policy challenges.
* We accept privacy is a real issue, but there are solutions.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

For further information

* Joe Urli
  President
  ACUO
  Email: president@acuo.org.au

* Brad Mason
  Secretary
  ACUO
  Email: secretary@acuo.org.au

Website: www.acuo.org.au

Copyright. Reproduction and redistribution not authorised without written permission from ACUO

Acknowledgements

* ACUO acknowledges the assistance of Peter van Blyenburgh, President of UVS International, and Peter La Franchi, UVS International Head of Mission in Australia, in the preparation of this submission.

Copyright. Reproduction and redistribution not authorised without written permission from ACUO