Submission to National Data Security discussion paper

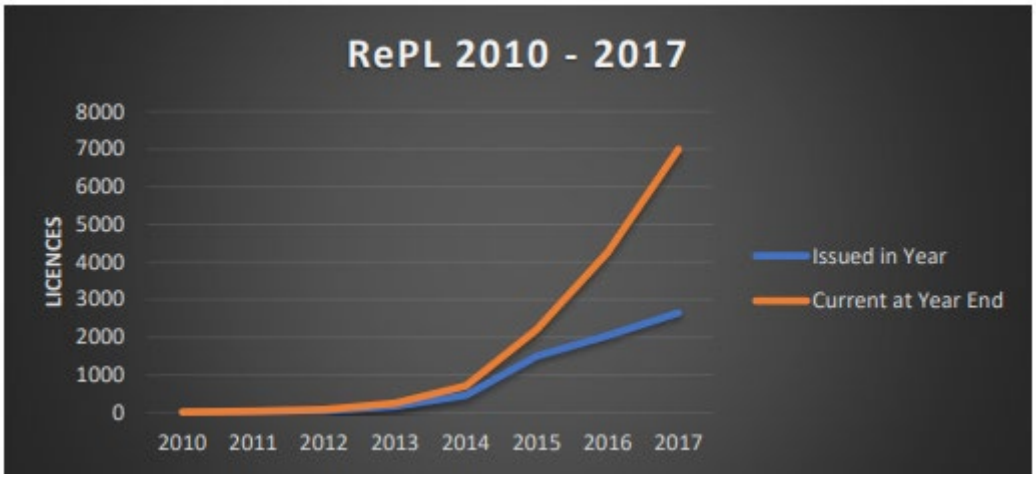
23 June 2022

Dear Panel,

By way of a brief introduction, Dr Gavin Mount is a senior academic from the School of Humanities, Arts and Social Sciences, University of New South Wales (Canberra) and David Beesley is a PhD candidate and Technical Services Manager with the School of Media and Communication and School of Design at RMIT University (Melbourne). Our current work involves situating humans within complex scenario-based interpretation dilemmas, recognising that individuals are increasingly 'quantified' and digitally enmeshed in today's data driven society.

We would like to highlight the importance of considering the potential Data Security implications relating to the proliferation and mass deployment of autonomous, semi-autonomous and automated vehicles across all domains (air, land, and sea), sectors, and segments of Australian society. Using aerial consumer drones as an example, industry estimates provided to the domain regulatory authority, CASA, suggest that there are well in excess of 150,000 drones – or 'Remotely Piloted Aircraft' [RPA] – currently in Australia. RPAs are used across a multitude of sectors including agriculture, mining, infrastructure assessment, search and rescue, fire and policing operations, aerial mapping and scientific research (Civil Aviation Safety Authority, 2018). Comparatively, the American FAA recently reported that they have exceeded one million RPAs in their registration system.

CASA continues to see exponential growth in the number of remote pilot licences [RePL] and remote operator certificates [ReOC] being issued.



NUMBER OF REPL IN AUSTRALIA 2010 - 2017

As at the 26 February 2018, there were:

- 7,380 remote pilot licence holders
- 2,342 RPA operator certificate holders (Civil Aviation Safety Authority, 2022)
- 10,253 online notifications from commercial RPA operators intending to undertake RPA operations in accordance with the standard RPA operating conditions – since the introduction of the RPAS notification system for excluded category RPA operators in September 2016 (Civil Aviation Safety Authority, 2018, p. 19)

In a medium uptake scenario, Deloitte Access Economics predicted commercial drone use across a number of sectors would expand Australia's GDP in 2025 by $1.5b; 2030 by $5.5b and 2040 by $14.5b. Commercial drone applications sectors considered by Deloitte in their report were listed as:

- Aerial photography
- Aerial patrol (e.g. border control and public safety)
- Precision agriculture
- Emergency management
- Photogrammetry, surveying, asset inspection and other GIS applications
- Construction/real estate images and monitoring
- Infrastructure monitoring
- Film making and other media uses
- Oil and gas exploration
- Weather forecasting and meteorological research
- Mail and small package delivery (Deloitte Access Economics, 2020)

Globally, the drone services market is expected to grow to $63.6 billion by 2025. Total global shipments of enterprise drones, defined as all unmanned aerial vehicles (UAVs) sold directly to a business for use in its operations, are predicted to reach 2.4 million in 2023 – increasing at a 66.8% compound annual growth rate. Drone growth will occur across five main segments of the enterprise industry: Agriculture, construction and mining, insurance, media and telecommunications, and law enforcement (Insider Intelligence, 2022).

Increasingly and in parallel, what is generically referred to as "swarms" of remotely controlled or autonomous drones are also becoming more common. In the foreseeable future, we expect these multi-element systems to become more prominent in recreation and entertainment as well as critical sectors such as service delivery, construction, agriculture, resource industries, utility maintenance, asset inspection, GIS, and public safety. As these systems become more enmeshed in our society, it is crucial that certain standards and regulations be put in place particularly regarding their data link and data acquisition capabilities, and the subsequent – and often cloud based – processing and storage of the acquired data.

> *Every government and every aviation safety regulatory authority in the developed world today is challenged by the growing number of still largely unanswered questions about the nature and magnitude of the risks associated with growing numbers of increasingly sophisticated RPAS technologies, coupled with effectively unfettered access to those technologies and devices, and the ease with which these can be used – responsibly and otherwise – in a variety of ways by virtually anyone.* (Civil Aviation Safety Authority, 2018, p. 6)

This projected exponential growth of aerial drone use across all sectors requires regulatory oversight above and beyond work CASA is already undertaking. Mitigation strategies should consider including comprehensive education, training, and professional development tools around the specific and thorny issue of data security when applied to autonomous, semi-autonomous and automated drone platforms.

CALL FOR VIEWS: BUILDING A COMMON UNDERSTANDING

1. What do you consider are some of the international barriers to data security uplift?

The impending proliferation of swarms in cities will generate significant amounts of geolocation and usage data. Internationally sourced hardware and software may not comply with domestic data security principles and practices. Swarm agents may encode nefarious elements within its algorithm, elements that may include facial or voice recognition data, persistent geo-location tracking (e.g. Uber) and 'default' privacy agreements (a.k.a. surveillance agreements) that permit the storage of data offshore.

2. How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

The EUGDPR document enshrines useful principles, however drone assemblages need to be considered in terms of hardware, software and the datalink. CASA regulates the usage of the hardware, however the hardware itself is potentially a data security issue. In the United States the degree of trusted assigned to drone hardware is determined by whether it has been 'Blue Listed' or 'Red Listed' by the US military. Blue Listed drone platforms are deemed to be trusted and are entirely indigenously manufactured with some notable exceptions such as the granting of "Blue Listing" to Parrot, a French consumer drone manufacturer. Conversely "Red Listed", or non-trusted drone platforms currently include any drone manufactured by the Chinese based electronics company DJI specifically due to the perceived data security issues with flight information stored on Chinese servers by default. For internet connected electronic devices the country of origin / country of manufacture needs to be listed on the packaging down to a component level. Software and NetWare that stores data should be required to have opt in/out protocols, with the default set to 'opt out' to encourage reflection by the end prior to opting in. Trusted hardware platforms could be certified, licenced, and accredited; non-trusted platforms should be flagged as such. Software should comply with national data protection acts and regulations.

3. What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?

We believe that data security needs to be identified as a national research, education, and outreach priority. Our emphasis would be on expanding research into human-data interface digital decision making in complex environments. Government support to develop scenario-based simulations would help understand the challenges facing data-enmeshed individuals, societies and also would be a useful tool for decision makers. A digital twin that explores notions of 'trust' in the age of machine learning and AI, if you will.

Problem-based learning in simulated education is used in Air Traffic Control [ATC] emergency and aviation event-based education to develop autonomous responses for the defender agents such as air traffic controllers, pilots, and other operators (Turhan, et. al. 2020). The aviation environment is data-rich, precise and requires real-time and on-the-job training for unexpected events. Scenario-based simulation education and training is one of the best solutions for airspace operators who must communicate, coordinate and make rapid, safe and correct decisions in a data rich, high-tempo

environment (see Cox, 2010). Informed end-users combined with resilient operators and processes are the key aspects of the highly complex, safety sensitive, high-risk and high-cost environment.

4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market?

5. Does Australia need an explicit approach to data localisation?

We recognise the complexity of this question requires situating the relationship between data, spatiality and citizen rights within a broader sociopolitical analytical framework. Informed by contemporary research and recommendations (Thrift, 2005; Lupton, 2016 and Zuboff, 2019), we agree that current self-tracking and data-capturing technologies have over-reached posing a potential danger to human liberty, autonomy and wellbeing. Data localisation has the potential to erode Australian democracy from within by reducing a capacity for autonomy, critical thinking and moral judgement. The globalised capture of this data threatens to undermine our democracy externally as it generates unprecedented concentration of knowledge primarily by large multinational corporations. Australian citizens need to have greater control over this data and we require "new laws and regulatory institutions that specifically address the mechanisms and imperatives of surveillance capitalism" (Laidler, 2019).

GOVERNMENT'S ROLE – FEDERAL, STATE AND TERRITORY AND MUNICIPAL GOVERNMENT UPLIFT

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

Data security is a national issue and as such requires a harmonised approach across all jurisdictions.

7. Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?

The reality in this connected digital world is we all need to take responsibility, and education is key. In the aerial drone sphere, CASA is the domain regulatory authority but requires help and expertise regarding the nuances and complexities of data protection. CASA recognises that social issues such as privacy concerns and data security are outside of their present scope and jurisdiction.

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

Regulatory uncertainty creates systemic problems for business and potentially stifles both innovation and investment. The current patchwork approach to data security creates the potential and opportunity for significant security 'gaps' in an increasingly connected digital world.

CLARITY AND EMPOWERMENT FOR BUSINESS

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?

The proliferation of drone usage creates concerns akin to those of IoT devices. Public information needs to be created based upon real-world case studies. Case studies should include geolocation data provided by sports watch and fitness bands, consumer drone platforms, mobile telephony and sat nav devices. Case study analysis can be used explore the potential risks associated with connected devices and the rise and rapid evolution of the Internet of Things [IoT].

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? (for example, a 'size' threshold).

The National Data Security Action Plan states (page 10) that data security is a collective responsibility, as such guidance and education should be as broadly encompassing as possible, especially with the rise of SME's or solo practitioners in the digital economy. For example, the 7,000+ licenced drone pilots within Australia, where the data stream and data acquisition is the main concern. Many commercial drone platforms store data by default on servers located offshore, with the potential to build large data sets, which could then be used for a variety of purposes without the data creator's consent include the training of machine learning [ML] and AI algorithms.

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

Reform and adoption require legislative clarity and support for changing the corporate culture. Regulation and bureaucracy are required but should not be so overwhelming that it confuses the message and stifles decision making and planning. Data users and data creators need to be engaged with, and listened to, in an ongoing conversation in this constantly evolving and highly dynamic space. Pragmatic factors such as cost, labour and time for implementation need to be considered from a business and small business perspective, which opens the possibility of additional incentives being required from the Government to encourage both participation and compliance.

EMPOWERING AND EDUCATING CITIZENS AND CONSUMERS (THE COMMUNITY)

14. Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

Some of the work in this space has already implemented by CASA who have begun a process of educating consumers and SMEs around regulations pertaining to consumer drones. Academic research on digital enmeshment could be leveraged to produce expert advice and develop real-world scenario simulations. Our hermeneutic framework (Mount & Beesley, 2022) is being employed in simulations designed to support analysts and operators interpret complex threat scenarios and design appropriate and proportionate responses. Education should also focus on empowering data creators and data users.

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

Accountability and trust could be enhanced with clearly articulated incentives and sanctions. Uncertainty surrounding the mechanisms can erode confidence. Over complicated regulation mechanisms could overwhelm and undermine compliance rates.

Public trust could also be improved with an extensive educational campaign around the risks of data stored offshore designed to empower individuals to determine 'sensitivity' and risk of their data exposure and to guide appropriate and informed measures. Professional development and education could also build accountability by improving the capacity for hermeneutic analysis of risk and threat assessment.

In an ever-changing world, the real challenge when considering data security is that data acquisition and processing occurs in a highly volatile and rapidly evolving space. As such any framework needs to be dynamic and scalable to account for the next technological 'thing' in whatever form that may take, and regularly reviewed at five-year intervals – or less – to accommodate or adapt to the associated new data security threats that will inevitably emerge.

Sources:

Civil Aviation Safety Authority. *Review of aviation safety regulation of remotely piloted aircraft systems* (2018). Canberra: Commonwealth of Australia.

Civil Aviation Safety Authority. *Remotely Piloted Aircraft Operator's Certificate (ReOC) holders | Civil Aviation Safety Authority.* (2022, May 29). Retrieved from Civil Aviation Safety Authority: https://www.casa.gov.au/search-centre/remotely-piloted-aircraft-operators-certificate-reoc-holders

Cox, Brenda A. *Scenario Based Training in an Aviation Training Environment*. (2010) All Regis University Theses. 2. https://epublications.regis.edu/theses/2

Deloitte Access Economics. *Department of Infrastructure, Transport, Regional Development and Communications - Economic Benefit Analysis of Drones in Australia.* (2020). Brisbane: Deloitte Access Economics. Deloitte Touche Tohmatsu.

Dept of Home Affairs, *National Data Security Action Plan* (2022) https://www.homeaffairs.gov.au/reports-and-pubs/files/data-security/nds-action-plan.pdf

Insider Intelligence. *Drone market outlook in 2022: industry growth trends, market stats and forecast.* (2022, April 15). Retrieved from Insider Intelligence:

https://www.insiderintelligence.com/insights/drone-industry-analysis-market-trends-growth-forecasts/

Laidler, John (2019) "High tech is watching you", *Harvard Gazette, (*March 4) https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

Lupton, D. (2016) *The Quantified Self,* Polity

Sinha, Vikram. (2022) *Platform Governance Through an Economic Lens.* Platform Governance through an Economic Lens - Centre for International Governance Innovation (cigionline.org)

Thrift, N. (2005) *Knowing Capitalism*, Sage

Turhan, U., Açıkel, B., Güneş, T. Hava (2020) "Emergency Management Simulation Practices with Problem Based Learning Method in Air Traffic Control Training: Theoretic Approach", *Journal of Aviation* 4: 147-161 https://dergipark.org.tr/en/pub/jav/issue/55074/713537

Zuboff, S. (2019) *The Age of Surveillance Capitalism*, Profile

Author Bios

Dr Gavin Mount is the Associate Head of School (Research Training) at the School of Humanities and Social Sciences. His primary area of research is in the application of critical security theories at the intercession between ethnic conflict and geopolitics. Recent publications include "Hybrid Peace/War" (2018), "micro-targeting" (2020) and "Nationalism" (2022). He has been a commissioning editor of *Australian Outlook* since 2017 and co-leader of a large UNSW Community of Practice on Student Wellbeing. The recipient of two Teaching Awards (2010 and 2020), he is widely recognised as an innovative leader in pedagogy of online engagement and simulations.

g.mount@unsw.edu.au ORCID ID

David Beesley is a media professional, documentary film maker, and technical services & facilities manager for the School of Media and Communication and School of Design (College of Design & Social Context) at RMIT University. He is presently completing his PhD 'Head in the Clouds: documenting the rise of personal drone cultures', which is a project-based longitudinal ethnographic documentary examining the significance of drone cultures in Melbourne. The School of Media & Communication hosts the ARC for Automated Decision Making & Society (ADM&S) (https://www.admscentre.org.au/); the RMIT / ABC FactLab; DERC (Digital Ethnographic Research Centre); and the cutting-edge NAS Media Precinct.

david.beesley@rmit.edu.au ORCID ID