Australian Attitudes Towards Privacy of Information: Will COVID-19 Make a Difference?

Leah Shanley, Michael N. Johnstone, Michael Crowley, Patryk Szewczyk

Australian Attitudes Towards Privacy of Information: Will COVID-19 Make a Difference?

Leah Shanley, Michael N. Johnstone, Michael Crowley and Patryk Szewczyk

School of Science, Edith Cowan University, Western Australia

Abstract. There has always been tension between security needs (as expressed by a nation-state) and privacy needs (as expressed by the citizens of said nation-state). Achieving this balance is perhaps one of the goals of statecraft. Terrorist attacks tend to shift the balance towards security, whilst proponents of civil liberties tend to want to move the balance in the other direction. We examine Australian attitudes to privacy in the light of the COVID-19 pandemic and consider whether the effect of the pandemic is likely to change Australian's perception of their fundamental right to privacy, as determined by law, enabled by technology and shaped by human concerns.

Keywords: Privacy, Surveillance, Security, Public Attitudes, COVID-19

1 Introduction

Security concerns have become heightened across Federal, State and Local government agencies alike, primarily due to the severity of international and domestic incidents that relate specifically to terrorism and cybercrime (ANZCTC, 2017). Terrorism incidents such as the attacks in the United States of America on September 11, 2001 and the Bali bombings in 2002, among others, have contributed to the growing use of surveillance technologies in both the private and public sectors (Mann & Smith, 2017). More recently, however, the COVID-19 pandemic has emerged and presented further privacy concerns for the public and privacy advocates. The COVID-19 response has seen an increase in the rapid deployment of surveillance devices in Australia. For instance, the use of drones and smartphone applications to enforce social distancing measures or support contact tracing methods.

The tension between privacy and security is a complex debate between privacy advocates and security proponents; however, public citizens appear to be either indifferent to, or are struggling to grasp, the effect of technological advancements on privacy erosion, especially when privacy infringements are legitimised when contextualised with the War on Terror (Broek, Ooms, Friedewald, Lieshout, & Rung, 2017) and more recently the COVID-19 pandemic. The introduction of public surveillance systems and laws that support their use appear contradictory. Juridical matters bring forth legal implications in relation to data handling, leaving little room for redress with the continued trend of surveillance systems as a remedy to support national security objectives.

This paper examines the privacy-security debate through the lens of the power model developed by Turner (2005). The balance between privacy and security is at the nexus of technology, law and people. Technology enables what is legitimate under law on

behalf of the people. Australians are typically mistrustful of their government with respect to personal data (Lupton, 2019) - they do not like to be identified. A recent survey by the Office of the Australian Information Commissioner (OAIC) showed that this is still an issue for Australians (OAIC, 2017). Witness the "Australia Card" of the 1980s and the more recent "My Health Record" (an opt-out system). Briefly, the Australia Card was a failed attempt to issue a national identity card. Further, approximately 20% of Australians have elected to opt-out of My Health Record. As noted by Hanson (2018), "The controversy over police access to the My Health Record [data] and the need to add further privacy protections in that scheme also point to heightened public awareness and concern about digitisation processes, including about losing control of personal information that might be used to cause harm". The 2017 survey administered by the OAIC showed that government access to personal data continues to concern Australians (OAIC, 2017). The COVID-19 pandemic may prove to be an interesting confounding variable. The use of Bluetooth Low Energy (BLE) technology, in the case of the COVIDSafe application (Department of Health, 2020) appears at first glance to potentially enhance the rapid detection of contacts with an infected person - a laudable public health goal. However, a BLE signal could produce false positives which would hinder, rather than help, the public health effort. Standing outside a closed office for 15 minutes could generate a "contact" where no direct exposure has occurred. This paper hereafter summarises related work on privacy, provides an extensive discussion of legal, technical and human-centred matters pertaining to privacy, shows how the discourse fits an established theory of power in groups (Turner's TPT) and concludes by suggesting that further work can be done in the form of surveying segments of the population to determine if the attitudes of Australians have changed.

2 Related Work

Privacy is recognised in fundamental documents that define human rights (Clark, 2006). For example, section 12 of the Universal Declaration of Human Rights states "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (UN General Assembly, 1948). Historically, Australians have been at best, reluctant to accept government attempts to impose policies that result in universal identification. In the 1980's the Hawke Government proposed introducing a national identity card (Hawley, 2005) that was quickly consigned to the waste bin of history. Recently, the Morrison Government's COVID-19 application attracted greater acceptance with citizens notwithstanding ongoing technical issues and release of draft legislation to enshrine privacy protections. While this draft legislation seems to exclude the operation of other security legislation the fact remains that Australia's security apparatus has acknowledged that it does at times carry out illegal acts in the course of fulfilling its role in protecting Australians (Moorhouse, 2014). If nothing else Australians are on notice that different Australian agencies hold different approaches to the balancing act that underpins the relationship between privacy and security.

The balance between privacy and security is continually shifting and increasing discord between individual privacy rights and the collective security objectives of a nation state (Mann & Smith, 2017). Goggin et al. (2017) conducted a survey of 1,600 Australians. The research explored questions about the nature of digital rights and covered four key issues, namely; (1) privacy surrounding data profiling and analytics, (2) government data matching and surveillance, (3) digital privacy relating to the work place (work), and (4) freedom of expression (speech) with an emphasis on online digital platforms (Goggin et al., 2017). Key areas of interest drawn from the research were the findings relating to privacy profiling, and government data matching and surveillance. The research revealed that Australians are genuinely concerned about their online privacy in agreeance with research conducted by the OAIC in 2017 that showed similar outcomes (OAIC, 2017). 65% of participants felt they had nothing to hide, whilst 67% actively took steps to protect their online privacy. 57% of participants agreed that corporations were a threat to privacy. With regards to government data matching and surveillance, 47% were concerned about government violating their privacy, however, when questions were framed from a security perspective the percentage changed. When respondents were asked whether they are in favour of law enforcement or security agencies accessing meta data, 42% were in favour, conversely, when framed as an anti-terrorism measure 57% were in favour (Goggin et al., 2017). The change in attitudes suggests that personal views towards privacy breaches varied depending on the context–further highlighting the complexity of the issue.

A 2017 survey on Australian attitudes towards privacy conducted by the OAIC (2017) further identified that 93% of respondents do not want their personal data sent and stored overseas. The desire for personal privacy has seen an increase in the use of encryption technology by consumers and enterprises globally (Korolov, 2016). The widespread use of encryption has contributed to more recent developments in law, for example, in 2018 the Australian Parliament passed the Assistance and Access Act 2018 (Cth). The Act is designed to improve the ability of Australian law enforcement and security agencies in decrypting information when investigating serious crimes (The Parliament of the Commonwealth of Australia, 2018). Thus, the introduction of the Act is a contributing factor to the rising tensions between privacy advocates and security proponents. Similarly, the Identity Matching Services Bill (2019) implements the Intergovernmental Agreement (IGA) on identity matching services. Under the Intergovernmental agreement, the Commonwealth and all states and territories agree to preserve or introduce legislation to support the sharing of facial images and related identity information via a set of identity-matching services (Parliament of Australia, 2019). While privacy laws in Australia do exist at both State and Federal level, not all government agencies work in unison, furthermore, juridical issues greatly influence law enforcement. As noted by Greenleaf (2020) any COVID-19 legislation needs to avoid 'pseudo-voluntary' compliance by which voluntary uptake becomes de facto compulsory. That is, any resultant legislation should make the uptake of the COVID-19 application 'genuinely voluntary and guaranteed by enforceable laws.' (Greenleaf, 2020). In contrast, the exposure draft makes it an offence to 'require another person to download the application or have the application in operation (The Parliament of the Commonwealth of

Australia, 2020b). The exposure draft does not use the words ‘voluntary’. Section 94B (Object of this Part) could enshrine the principle of voluntary uptake.

3 Discussion

Paine et al. (2007) noted over a decade ago, that advances in technology have altered the way in which information is collected, stored and exchanged. Increasing threats to public safety, whether criminal or health related, have contributed to the accelerated implementation of surveillance technologies in both the public and private sector. An outcome is that regulators are struggling to keep abreast of technological developments and their impact on society (Mann & Smith, 2017). Public trust, a domain of concern, is found to play a critical role regarding surveillance in society. Major studies, for instance, the Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action (PACT) survey, found that respondents level of distrust reflected in the preferences for different security and privacy practices (Patil et al., 2015). The Australian Government is not exempt from public trust issues on multiple fronts. For example, the government’s handling of the Robo Debt process wherein its use of flawed technology (Price, 2019) to shift the onus of proof of financial entitlement onto those least able to look after themselves indicated either a collective lack of trust in citizens or an unhealthy focus on achieving a budget surplus at all cost.

In a not unrelated vein, the government’s pursuit of journalists and whistle-blowers who, respectively, exposed government plans to secretly spy upon Australians (Ryall, 2019; Tillett, 2018) and revealed illegal government behaviour against a friendly neighbour during Timor Gap negotiations (Knaus, 2019; Heathcote, 2013) further illustrates a preoccupation with secrecy. Furthermore, the government has just introduced into parliament proposed amendments to the Australian Security and Intelligence Act 1979 (Cth) (ASIO Act). These amendments include provision for ASIO to use non-intrusive surveillance devices on Australian citizens without needing to apply to a court for a warrant and to examine articles being delivered by a delivery service provider (The Parliament of the Commonwealth of Australia, 1999). These proposed amendments have been described as ‘one more step towards a totalitarian state’ (Barnes, 2020). This same government now asks Australians to trust it on providing adequate protections of citizen’s privacy within its COVID-19 smartphone application. This is the same application that has not achieved universal uptake by all federal politicians, including some ministers of the government (ABC News, 2020). Importantly, one politician has given the protection of the identity of whistle-blowers as the reason why he will not download the COVID-19 application. This raises an important issue, while the draft legislation provides criminal sanctions for misuse of ‘tracing application data’ beyond medical contact tracing for the purposes of COVID-19, the derivative use of the outcome of such tracing might not be so easily prevented. It might not take much for a well-resourced agency to link a person of interest or to narrow its field of search to persons required to isolate following the identification of a politician, investigative journalist or lawyer who has become a recent victim of COVID-19. For clever people, knowing where to start looking is almost as good as knowing where to search.

Brown, Vandekerckhove, and Dreyfus (2014) confirm that transparency is indeed important to the public in Australia and the UK, thus public trust relies on increasing the responsibility of institutions to recognise and protect whistle-blowers. Brown, Vandekerckhove, and Dreyfus (2014) show in their research regarding transparency and whistleblowing, that public attitudes towards whistleblowing is divided. Half of the respondents (50%) surveyed felt information was kept to secret demonstrating public opinion in these domains has the potential to impact political support. Therefore, introducing intrusive means of data collection in combination with legislative amendments that threaten public trust is paramount. As such public figures, for example, Julian Assange, have potential to not only influence public opinion but contribute to the increasing pressure of trust in modern institutions.

Recent developments with respect to COVID-19 have prompted governments of the world to canvas technological solutions capable of contributing to the response effort. For instance, drone deployment has been trialed in some countries to enforce social distancing polices while other technological solutions such as GPS ankle monitoring devices have been acquired to help police track citizens who should be in quarantine or self-isolation (Sky News, 2020). In contrast, automatic number plate recognition (ANPR) cameras have been purchased in the state of Western Australia to enforce statewide travel restrictions (Hendry, 2020b). Mann and Smith (2017) astutely point out that Australia is following the trend of expanding its surveillance capabilities, noting the most significant development that occurred in 2015. The National Facial Recognition Biometric Matching Capability (NFRBMC) was announced and intended to become operational in 2016. The NFRBMC provides for the sharing of facial templates across state and federal agencies. According to more recent reports, Western Australia as a case in point, at present is preparing for the upload of licence and photographs to be shared, while other states (Victoria, South Australia and Tasmania) have already supplied driver's licence details and photographs to the National Driver's Licence Facial Recognition System (NDLFRS) (Hendry, 2020a). The NDLFRS, hosted on a Department of Home Affairs platform, contributes data to the NFRBMC system. The end result will probably result in the driver's licence becoming by stealth what Australian's had collectively rejected with the Hawke Government (the national identity "Australia" card). A government focused on identification and secrecy may find the lure of surreptitiously linking such data to Australians using the same phone application very tempting.

One particular technological response measure of interest is the introduction of a smartphone application for the purpose of social distancing and contact tracing. Countries around the world such as Singapore, Israel, South Korea and the United States have adopted surveillance methods leveraging mobile location data to enforce social distancing policies and contact tracing (Ng, 2020). Contact tracing aims to identify citizens that have come into close contact with a COVID-19 positive case or who have tested positive, thus the data can be used to promptly notify people who may be at risk or should be in quarantine. The COVIDSafe application, released in Australia on 26 April, 2020 (Department of Health, 2020), underwent some consultation prior to its release. The Department of Health released a Privacy Impact Assessment (PIA) prior to the application being released that documented recommendations yet to materialise.

In addition, the PIA performed a compliance analysis against the Australian Privacy Principles (APPs). Whilst there are rhetorical moves to enforce penalty for breach of information privacy (Dentons, 2019), it is important to note that the APPs are not enforceable (Australian Law Reform Commission, 2014, p. 21), in other words, legal remedy for encroachment does not currently exist in Australia. Furthermore, the Australian Privacy Act (that incorporates the APPs), provide exemptions to a number of Federal and State agencies, thus it is questionable as to what protections exist for the Australian public should a breach be realised.

As the privacy debate continues, there exists an emerging discourse with regards to public surveillance and security, or put another way, national security versus information security. The balance between privacy and surveillance for the purpose of national security - a debate that continues to gain ground, demonstrates the discourse with the introduction of Acts such as the Assistance and Access Act (2018), designed to improve the ability of Australian law enforcement and security agencies in decrypting information, is in contradiction to the advocacy of privacy. The Australian Government purportedly promotes privacy on the one hand while simultaneously implementing legislation that supports intrusive means of data collection. The primary legislation for regulating privacy in Australia is the Privacy Act 1988 (Cth). The Australian Privacy Principles (APPs), included in schedule 1 of the Privacy Act, outline how personal information should be managed and handled by entities subject to the Act. Exemptions to the Act include entitles with an annual turnover of less than three million AUD, local and state governments are also exempt (OAIC, n.d.). In addition, defence and intelligence agencies are either partially or completely exempt (Australian Law Reform Commission, 2008). The Australian Law Reform Commission (2008) stated that “Australia is yet to achieve uniformity in the regulation of personal information”.

Due to public concern, Australia’s Federal Health Minister, Greg Hunt, shared a Determination under the Biosecurity Act 2015 (Cth) in an attempt to protect people's privacy and quell fears. The Determination restricts access to state and territory health authorities only, for the purpose of contact tracing. The Determination declares that a person must not retain the data on a database outside Australia, and the Commonwealth must cause COVID-19 application data in the National COVIDSafe data store to be deleted after the COVID-19 pandemic has concluded (Australian Government, 2020). A better option would be to insert a sunset clause in the proposed legislation requiring the approval of parliament to extend the use of the COVID-19 application legislation notwithstanding a Determination can be amended or appealed at the discretion of the government anytime. Thus, the finalisation of the draft COVID-19 application legislation is crucial for clarity. As legal experts have warned, legislation would be a better instrument (Bogle, 2020). Law Council of Australia president Pauline Wright stated, “there was some potential legal ambiguity around whether laws authorising the law enforcement and intelligence warrants could override the Determination's prohibition on access” (Bogle, 2020). In addition to the ambiguity that exists in Australian law, international requests for data deserves the serious consideration of the current Parliamentary Joint Committee on Intelligence and Security (PJCIS) review. To illustrate further, the Department of Health has contractual agreements with Amazon Web Services (AWS) for the COVIDSafe application data store. The use of AWS, an American

company, raises some juridical issues. AWS has an annual turnover of more than three million AUD qualifying AWS as an APP entity. However, a bilateral agreement between Australia and the United States following enactment of the United States CLOUD Act (Clarifying Lawful Overseas Use of Data), enacted in 2018, may or may not weaken protections afforded under Australian's Privacy Act. This agreement is subject to the outcome of the PJCIS review and is currently being negotiated (see Second Reading Speech on the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 by Minister Mr Tudge (Parliament of Australia, 2020). In the meantime, The PJCIS has commenced a review into the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 with a reporting date of 26 June 2020 (The Parliament of the Commonwealth of Australia, 2020a). As recently as 14 May 2020, Taylor (2020) has canvassed concerns about US law enforcement accessing COVID-19 data making the PJCIS review crucial for those concerned with privacy.

Another issue worthy of consideration is the Archives Act 1983 (Cth), an Act that sets out requirements for the retention of data. This means that archived data needs considerable attention in relation to data access, storage, backups and retention timeframes. Other pertinent issues worthy to note include function creep and exemptions to current Australian law. Function creep in generic terms addresses the originally intended purpose of a particular surveillance system. The originally intended purpose does not necessarily mean the surveillance technology will cease to operate once the originating use case ceases. A case in point is the COVIDSafe application. Whilst the Australian Government has stated that the data store must be deleted when the pandemic ends, as noted by Ahmed et al (2020), the term "end of pandemic" is vague. Whilst use of the technology by the government of the day may have well-deserved intentions, this does not guarantee future governments will hold the same values. Therefore, legislative guarantees to protect against a host of potentially lucrative markets or temptation of the security apparatus (both public and private) require mitigation to balance the potential unforeseen effects or secondary uses.

Turning to the implication of exemptions, certain Australian laws such as the Privacy Act 1988 (Cth) allow for state and federal exemptions across agencies. Should Pauline Wright's concerns come to fruition, laws that authorise state, federal and intelligence agency warrants override the Determination's prohibition on access, therefore, requirement for entities to share information with foreign governments exists and requires rigorous investigation, fortunately this is currently part of the PJCIS review mentioned above.

Instruments to investigate data protection and information privacy are widely available. PIA's are one such mechanism designed to consider the impacts and issues that may arise due to deployment of surveillance systems, In addition, PIA's aim to bring forth alternatives or safeguards to mitigate negative impacts to stakeholders (Wright et al., 2010). The PIA officiated by the Department of Health failed to adequately address these issues relating to the COVIDSafe application data. The PIA raised concerns in the form of recommendations prior to release. However, until legislation concerning usage and contractual arrangements is enacted, information privacy related matters will continue to emerge. Moreover, public trust will continue to decline. It is not desirable

that a PIA for an application critical for the health and safety of Australians, and by extension privacy, did not seek independent expert or community input prior to release. The Australian government has openly stated that returning to normal life is dependent upon the application being downloaded and used (Ruiz and Moore, 2020). In contrast, Professor McLaws, a member of the WHO coronavirus response panel stated "What's not clear is who the custodian of the data is and where the data are stored. It's not true informed consent" and in another statement "Until we know what the source code is and until we know whether Amazon has to fulfil Australian law, I won't download the application" (White, 2020). Amazon's relationship with Australian law in releasing data held within Australia to the United States of America will hopefully crystallise after the PJCIS review into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 is completed.

Privacy of one's information is significantly important in the pursuit of public trust, a critical factor that may impact on citizens' support for a security practice (Friedewald, van Lieshout, Rung, & Ooms, 2016), thus acceptance of intrusive technological solutions rely heavily on trust in the institutions that advocate such practices. The aim of the Privacy and Security Mirrors: "Towards a European Framework for integrated decision making" (PRISMS) project, was to gain better understanding of the relation between surveillance, security and privacy that could inform public policy and decision makers. The PRISMS project, a relatively large study, found a strong correlation between public trust and privacy intrusive measures, thus public trust played a critical role in the acceptance of security practices (Friedewald et al., 2016). The introduction of the General Data Protection Directive in May of 2018, otherwise referred to as the GDPR, illustrates that privacy of personal data is a serious issue in the European Union. The PRISMS project successfully informed policy makers in the EU, and by implication, influenced policy makers worldwide to follow suit (van Lieshout, Friedewald, Wright, & Gutwirth, 2013).

We acknowledge that any solution that enables health professionals to effectively and efficiently detect COVID-19 transmissions is a benefit to society as a whole and that contact tracing is effective. Conflicting views are however apparent with Norway's health authority for instance ceasing to use the country's COVID-19 application and deleting existing data (Kelio, 2020). Within Australia, there are concerns about the technical implications of the use of the COVIDSafe application. We have already suggested a scenario where a false positive might occur. Interesting, the OAIC recommends turning Bluetooth 'off' to preserve privacy (although the pandemic might be considered a special case). Perhaps more seriously, there have been reports of the application interfering with medical devices that also use Bluetooth. Bluetooth may also be resource-intensive and drain a phone's battery prematurely, so users might be reluctant to enable it, thus invalidating the data collected by the application. Furthermore, the application does not function correctly on Apple products. Notwithstanding the functionality issue, Apple and Google are jointly designing a different privacy-preserving contact tracing protocol. The Apple/Google solution is different to the COVIDSafe application in several respects, in that their solution does not collect location data from

a user's phone, nor does it share the identities of users with each other (or with Apple/Google for that matter). Further, random Bluetooth identifiers rotate every 10-20 minutes, which helps prevent tracking.

We now examine the above evidence and frame it in terms of Turner's Three Process Theory (TPT) of power. Turner (2005) contends that the "standard" theory of power is really a set of general assumptions about the relationship between power and influence. He addresses this by providing a more formal model of the factors that influence power (see figure 1). Turner's model is interesting in that, contrary to the standard model of power, group formation or the development of a shared social identity is the catalyst for influence, and this influence (separated by the different elements of persuasion, authority and coercion) is the foundation of power.

Applying Turner's TPT to the constructs of figure 1, we find evidence (or, at least the semblance) of a shared social identity (group formation), driven by the COVID-19 threat and expressed by frequent television advertising as "We are all in this together". Examining the three elements of influence, there is evidence of persuasion or convincing someone that your view is the correct one (advertising campaigns exhorting citizens to download the application), authority or the belief that someone else can control what you do (the government wants citizens to download the application) and coercion or someone can control your behaviour, even against your own interests (you may not be able to attend certain events if you have not downloaded the application). Notwithstanding concerns expressed about the security of the application's data and potential future uses (cross-matching) of said data, there is also an "appeal to the gallery" implicit in the conversation around Facebook and other social media platforms capturing more personal data than the application (therefore, why not use the application?). One could argue that end-user's perceptions of Facebook data collection processes are camouflaged through the perceived leisurely benefits of the application. Patil and Shyamasundar (2019) suggest that end-users believe they may exercise a degree of control over Facebook's data collection process, despite not actively reviewing or adjusting any controls. In contrast COVID-19 centric applications are often managed by the governing body thus minimising opportunities for end-users to exercise control. The final element of Turner's model, gaining control of resources, is evidenced by considering the data collected by the application to be a resource.

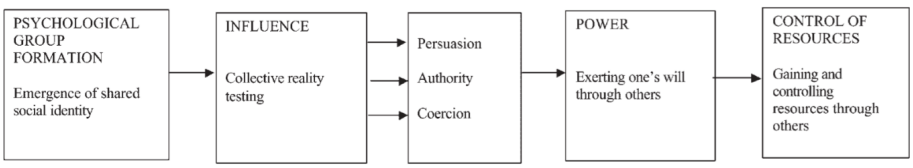

Fig. 1. Turner's Power Model (adapted from Turner, 2005).

4 Conclusion

The number of private and public sector organisations deploying surveillance technologies is increasing rapidly (Mann & Smith, 2017). This trend is expected to continue

as new challenges emerge, for example, the outbreak of COVID-19. Recent law developments, for example, the Identity-Matching Services Bill (2019) or the Assistance and Access Act 2018 (Cth), have generated significant concern in regard to the erosion of privacy. In Australia, the uploading of facial images and licence plate information to the National Database is now a reality with little oversight and little debate regarding the rollout of such technologies.

It is clear from the literature that privacy is important to the public. With the introduction of new surveillance methods such as the deployment of drones, GPS tracking devices and contact tracing apps, public concern will likely continue to increase. An important finding from the EU PRISMS project was that public trust was paramount. The research concluded that public trust played a critical role in the acceptance of security practices (Friedewald et al., 2016). If surveillance technologies are to be deployed as solutions to security objectives, or in the case of COVID-19, a rapid response to unforeseen circumstances, then the Australian Government has a responsibility to address the ambiguity that surrounds the public's perception of technological solutions and the laws that purport to protect privacy. A clear and definite roadmap for the reversal of intrusive technological surveillance systems would contribute to public trust, however such debate is absent from the discussion. The Australian Privacy Act offers little redress for breach of information privacy, moreover, the plethora of Acts, Bills and other Amendments provides for a contradictory landscape that is difficult to navigate leaving the average Australian often confused and mislead when new surveillance systems are introduced. It is time to consolidate these nuances surrounding law and design a solid framework for the deployment of surveillance technology. Worthy of consideration among all the newly, or otherwise predicated surveillance systems, is the continued advocacy of surveillance technology as a primary solution to national and state security objectives. The trade-off paradigm, that is, the assumption people are willing to trade privacy for more security, has been debated among scholars and academic circles for considerable time. People desire both security and privacy (Broek et al., 2017), thus finding the balance is pertinent in the pursuit of public trust. Friedewald, Lieshout, Rung, Ooms, and Ypma (2015) showed in research concerning the trade-off paradigm, evidence against the trade-off hypothesis and found no significant statistical correlation between people's valuation of privacy and security concern, therefore, generalising that Australian citizens are willing to trade privacy for more security is not consistent with the evidence.

We are not arguing that privacy trumps security in all cases. All nations keep secrets and it is in their national interest to do so. What we observe is that, by nature, Australians are reticent to share their personal information with any government entity. In order to test if this is true, we propose to undertake a survey of segments of the population to evaluate current Australian attitudes to privacy and to evaluate if the COVID-19 pandemic changes these attitudes in any significant way.

The COVID-19 pandemic has seen the suspension of parliamentary sittings potentially setting a precedent for future emergency protocols to be established. Laws have been passed without opposition and surveillance systems are in the process of rapid deployment, thus the absence of political safeguards reduces the potential for external

scrutiny. While the gravity of the pandemic can be appreciated, and we are indeed chartering unfamiliar waters, still it is unequivocally necessary that a well-informed sense of assurance that information risks and controls are in balance is paramount, in other words, a clear and concise Business Continuity Plan on behalf of Federal and State governments is crucial to enable continuation of government and democratic debate. Furthermore, decision making without practicing due diligence and regard for the impact on the Australian public deserves criticism. As stated by Zedner (2009) “Do we want to be completely secure in a police state?”.

References

1. ABC News. (2020). Easing coronavirus restrictions depends on the uptake of the Government's tracing app, so has your MP downloaded it? *ABC News*. Retrieved from https://http://www.abc.net.au/news/2020-05-07/has-your-mp-downloaded-the-coronavirus-tracing-app/12215092?nw=0
2. Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., . . . Jha, S. (2020). A Survey of COVID-19 Contact Tracing Apps. Ithaca: Cornell University Library, arXiv.org.
3. ANZCTC. (2017). *Australia's Strategy for Protecting Crowded Places from Terrorism*. Commonwealth of Australia Retrieved from https://http://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/Australias-Strategy-Protecting-Crowded-Places-Terrorism.pdf.
4. Australian Government. (2020). *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*. Retrieved from https://http://www.legislation.gov.au/Details/F2020L00480.
5. Australian Law Reform Commission. (2008). Australian Privacy Law and Practice (Vol. 3).
6. Australian Law Reform Commission. (2014). Serious Invasions of Privacy in the Digital Era.
7. Barnes, G. (2020). New ASIO law one more step towards a totalitarian state. Sydney Morning Herald, May 13. Retrieved from: (https://www.smh.com.au/national/new-asio-law-one-more-step-towards-a-totalitarian-state-20200513-p54smi.html
8. Bogle, A. (2020, April 27, 2020). Will the Government's coronavirus app COVIDSafe keep your data secure Here's what the experts say. *ABC News*. Retrieved from https://http://www.abc.net.au/news/science/2020-04-27/covidsafe-contact-tracing-app-coronavirus-privacy-security/12186044
9. Broek, T. v. d., Ooms, M., Friedewald, M., Lieshout, M. v., & Rung, S. (2017). Privacy and security: Citizens’ desires for an equal footing *Surveillance, privacy and security : citizens' perspectives*: Taylor and Francis, 2017-01-01.
10. Brown, A. J., Vandekerckhove, W., & Dreyfus, S. (2014). The relationship between transparency, whistleblowing, and public trust. doi: 10.4337/9781781007945.00008
11. Clark, R. (2006). What's 'Privacy'? .
12. Dentons. (2019). New tougher penalties to apply in Australia for breach of privacy. Retrieved from https://www.dentons.com/en/insights/alerts/2019/march/28/new-tougher-penalties-to-apply-in-australia-for-breach-of-privacy
13. Department of Health. (2020). COVIDSafe app [Press release]. Retrieved from https://http://www.health.gov.au/resources/apps-and-tools/covidsafe-app

14. Friedewald, M., Lieshout, M. v., Rung, S., Ooms, M., & Ypma, J. (2015). *Privacy and security perceptions of european citizens: A test of the trade-off model*. Retrieved from WorldCat.org database. Springer New York LLC.
15. Friedewald, M., van Lieshout, M., Rung, S., & Ooms, M. (2016). The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security *Data Protection on the Move* (pp. 51-74): Springer Netherlands : Dordrecht.
16. Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., & Bailo, F. (2017). Digital Rights in Australia.
17. Hanson, F. (2018). Preventing another Australia Card fail. Australian Strategic Policy Institute.
18. Heathcote, S. (2013). Australia and Timor Leste in The Hague. *The Conversation*.
19. Hendry, J. (2020a, March 27, 2020). WA prepares for national face matching database upload. *IT News*. Retrieved from https://http://www.itnews.com.au/news/wa-prepares-for-national-face-matching-database-upload-539863
20. Hendry, J. (2020b). WA to electronically track COVID-19 patients who defy isolation orders. *IT News*. Retrieved from https://http://www.itnews.com.au/news/wa-to-electronically-track-covid-19-patients-who-defy-isolation-orders-546224?eid=65&edate=20200414&utm_source=20200414&utm_medium=newsletter&utm_campaign=sc_weekly
21. Kelio, L. (2020). Coronavirus: Contact-tracing apps face further hitches. Retrieved from https://www.bbc.com/nes/technology-53051783
22. Knaus, C. (2019). Witness K and the outrageous spy scandal that failed to shame Australia. *The Guardian*. Retrieved from https://http://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia
23. Korolov, M. (2016). Study: Encryption use increase largest in 11 years. *CSO*. Retrieved from https://http://www.csoonline.com/article/3088916/study-encryption-use-increase-largest-in-11-years.html
24. Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *The University of New South Wales Law Journal, 40*(1), 121-145.
25. Moorhouse, F. (2014). *Australia Under Surveliance*, Sydney: Random House.
26. OAIC. (2017). Australian Community Attitudes to Privacy. Office of the Australian Information Commissioner. Retrieved from https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-2017-report.pdf
27. OAIC. (n.d). Government Agencies. Office of the Australian Information Commissioner. Retrieved from https://www.oaic.gov.au/privacy/your-privacy-rights/government-agencies/
28. Ng, A. (2020). Location data used for tracking COVID-19 has its limits, ACLU warns. *CNET*. Retrieved from https://http://www.cnet.com/news/location-data-used-for-tracking-covid-19-has-its-limits-aclu-warns/
29. Parliament of Australia. (2019). *Identity-matching Services Bill 2019*. Retrieved from https://http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6387.
30. Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (2020).
31. Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., & Robinson, N. (2015). Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey. PACT Project Consortium.

32. Patil, V. & Shyamasundar, R., K. (2019). *Is Privacy a Myth for Facebook Users?* Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019), pages 510-516
33. Price, J. (2019). Quiet Australians, it's time to ask Centrelink for your money back - loudly. *The Sydney Morning Herald*. Retrieved from https://http://www.smh.com.au/national/quiet-australians-it-s-time-to-ask-centrelink-for-your-money-back-loudly-20191128-p53f1i.html
34. Ruiz, K., Moore, C (2020). Missing the pub this arvo? Well download the COVIDSafe app and we'll open them up, Scott Morrison says. *Daily Mail Australia*. Retrieved from https://www.dailymail.co.uk/news/article-8276671/Australians-told-return-normal-life-soon-download-Covid-19-app.html
35. Ryall, J. (2019). Federal police raid home of Australian journalist who revealed government's proposal to spy on the public. *Business Insider*. Retrieved from http://www.businessinsider.com.au/federal-police-raid-home-of-australian-journalist-who-revealed-governments-plan-to-spy-on-the-public-2019-6
36. Sky News. (2020). Drones Deployed to police social distancing in WA [Press release]. Retrieved from https://http://www.skynews.com.au/details/_6145829434001
37. Taylor, J. (2020). Questions remain over whether data collected by Covidsafe app could be accessed by US law enforcement. Retrieved from: https://www.theguardian.com/law/2020/may/14/questions-remain-over-whether-data-collected-by-covidsafe-app-could-be-accessed-by-us-law-enforcement
38. The Parliament of the Commonwealth of Australia. (1999). *Australian Security Intelligence Organisation Legislation Amendment Bill 1999*. Retrieved from: https://www.legislation.gov.au/Details/C2004B00436/Revised%20Explanatory%20Memorandum/Text
39. The Parliament of the Commonwealth of Australia. (2018). *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 - Explanatory Memorandum*. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application/pdf.
40. The Parliament of the Commonwealth of Australia. (2020a). *Explanatory Memorandum: Telecommunications Legislation Amendment (International Productions Orders) Bill 2020 T*. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6511_ems_0ac5ae09-3e3e-400b-ae5e-680a68af4e45/upload_pdf/733176.pdf;fileType=application%2Fpdf.
41. The Parliament of the Commonwealth of Australia. (2020b). *Privacy Amendment (Pubic Health Contact Information)*. Retrieved from https://http://www.ag.gov.au/RightsAndProtections/Privacy/Documents/exposure-draft-privacy-amendment-public-health-contact-information.pdf.
42. Tillett, A. (2018). Top bureaucrats deny report cyber agency wants to spy on Australians. *Financial Review*. Retrieved from https://http://www.afr.com/politics/top-bureaucrats-deny-report-cyber-agency-wants-to-spy-on-australians-20180429-h0ze7a
43. Turner, J.C. (2005). Explaining the Nature of Power: A Three-Process Theory. *European Journal of Social Psychology* (35:1), January, pp 1-22
44. Universal Declaration of Human Rights (1948).
45. van Lieshout, Marc, Michael Friedewald, David Wright, and Serge Gutwirth. 2013. "Reconciling Privacy and Security." Innovation 26(1-2):119–19.
46. White, N. (2020). Australia's leading coronavirus expert at the World Health Organisation REFUSES to download the COVIDSafe app - despite Scott Morrison saying it's our key to lifting lockdowns, News. *Daily Mail Australia*. Retrieved from

https://http://www.dailymail.co.uk/news/article-8281393/Australian-Infection-expert-REFUSES-download-COVIDSafe-app.html

47. Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., . . . Bigo, D. (2010). Sorting out smart surveillance. *Computer Law & Security Review, 26*(4), 343-354. doi: https://doi.org/10.1016/j.clsr.2010.05.007
48. Zedner, L. (2009). *Security* Key Ideas in Criminology, 3, Retrieved from WorldCat.org database Retrieved from http://public.eblib.com/choice/publicfullrecord.aspx?p=425617