Privacy Concerns and Acceptance of Government Surveillance in Australia

Joel Kininmonth
School of Management
Curtin University
Perth, Australia
Email: joel.kininmonth@postgrad.curtin.edu.au

Nik Thompson
School of Management
Curtin University
Perth, Australia
Email: nik.thompson@curtin.edu.au

Tanya McGill
School of Engineering and Information Technology
Murdoch University
Perth, Western Australia
Email: t.mcgill@murdoch.edu.au

Anna Bunn
Curtin Law School
Curtin University
Perth, Australia
Email: a.bunn@curtin.edu.au

Abstract

Increases in routine data collection and surveillance in recent years have resulted in ongoing tension between citizens' privacy concerns, perceived need for government surveillance and acceptance of policies. We address the lack of Australia focussed research through an online survey of 100 Australian residents. Data was analysed using PLS, revealing that privacy concerns around collection influence acceptance of surveillance but do not influence enactment of privacy protections. Conversely, respondents' concerns about secondary use of data were unrelated to their levels of acceptance, yet were a significant determinant of privacy protections. These findings suggest that respondents conflate surveillance with collection of data, and may not consider subsequent secondary use. This highlights the multi-dimensional nature of privacy which must be studied at sufficiently granular level to draw meaningful conclusions. Our research also considers the role of trust in government, and perceived need for surveillance and these findings are discussed with their implications.

Keywords Privacy Concerns, Government Surveillance, Acceptance of Surveillance, meta-data retention, Australia

1 Introduction

In recent years, citizens in many jurisdictions have found themselves subject to increasing levels of routine government surveillance (Denemark 2012). This position is generally justified by policy makers as a necessary response to protect the population from criminal or terrorist activities. However, there is potential for these measures to lead to a perceived erosion of privacy. As an example, in Australia, the recently implemented metadata retention regime mandates that service providers log their customers' location data and online activities for a period of two years. This has broad reach and is of concern to many residents, potentially leading them to reject the justification for this collection, and/or to enact privacy protections to safeguard themselves.

Anecdotal evidence at various points in time supports this position. For instance, internet searches for privacy protections such as VPN or Tor increased immediately after Edward Snowden's leaks regarding government surveillance, and later after the implementation of the metadata retention legislation in Australia (Google Trends 2018a; Google Trends 2018b). This suggests that citizens may be responding to this perceived intrusion by considering means to circumvent such surveillance measures and protect themselves online.

Evidence from the US and Europe reveals several factors that can influence the public acceptance of surveillance measures: these include privacy concerns (Dinev and Hart 2006; Dinev et al. 2008), the perceived need for surveillance (Brown and Korff 2009; Dutton et al. 2005), trust in the government and its management of data (Trüdinger and Steckermeier 2017) and the use of privacy protections (Joh 2013). Despite this, there has been little research conducted in an Australian context as to the factors influencing public acceptance of government surveillance.

Our central research question is thus: What are the determinants of acceptance of government surveillance of the Australian public? We address the research gap by developing a model considering the factors that drive public acceptance of surveillance. We then empirically evaluate this model by gathering survey data from 100 Australian residents and analysing the results using Partial Least Squares (PLS) structural equation modelling. In the remaining sections of the paper we consider the background and justification for our hypotheses, followed by our data analysis and discussion of results. The paper closes by considering implications for both theory and practice.

2 Theoretical Framework and Research Hypotheses

Prior literature suggests that there is lack of systematic understanding of the public's view on government surveillance (Reddick et al. 2015; Robert 2015). In recent years, surveillance has been increasingly normalised, with multiple facets of daily life subject to increased scrutiny and "datafication". As noted, our literature review revealed that most work has been conducted in the US with little work situated in an Australian context. This is relevant, as national differences in legal frameworks, societal norms or even culture may influence the acceptance of government surveillance. Furthermore, the Australian metadata retention regime is one of the motivations for this study, as both the success and the acceptance of this significant and wide reaching project may hinge on some of the factors being considered in this research.

Whatever the ends served by government surveillance, public perceptions of government surveillance practices are important. As the Australian Law Council has recently observed in relation to proposed identity-matching legislation, the government should be "highly conscious of how the law is seen to operate and, in particular, maintain robust levels of transparency and accountability" (Bailes 2018). Dutton et al. (2005) explored the role of cyber trust in government. They identified a "trust tension" between the need to collect data on individuals as the basis for providing services, and anxieties about data surveillance or the inappropriate use of personal information gathered, stored, and analysed using information technologies. Through this exploration, they identified strategies which the government could employ in order to enhance the level of trust, including establishing identity, the implementation of guidelines and legal frameworks, and the importance of legislation being implemented in ways that enhance, rather than undermine trust. In this research, we study several potential determinants of this trust, or acceptance, including privacy concerns, perceived need for surveillance, and trust in the government and its management of data. The theoretical foundation of our research builds on the model developed by Dinev et al. (2008), which we extend with constructs from other related work (e.g. Siegrist et al. 2003; Trüdinger and Steckermeier 2017). The justification for inclusion of these constructs and the associated hypotheses are discussed in the following sections.

2.1 Privacy Concerns of Collection and Secondary Use of Data

Privacy as a concept has proven notoriously difficult to define (Smith et al. 2011), not least due to its multi-faceted and highly contextualised nature – that is, privacy means different things to different people and can be understood differently depending on where and when one is situated (e.g. Thierer 2013; Whitman 2003). Several overlapping categories, or domains, of privacy have been identified (Banisar and Davies 1999), including information privacy, territorial privacy, bodily privacy and privacy of communications. In terms of information privacy, Smith et. al (1996) identified key areas of privacy concerns held by individuals as including the collection of, improper access to, and unauthorised usage of information. In terms of internet privacy concerns, these have been identified (Dinev and Hart, 2006a) as "perceptions about opportunistic behaviour related to the disclosure of personal information submitted over the Internet", and it is these concerns that are at the forefront of people's minds. The general perception of threats to information privacy is in a gradual shift away from the threats posed by the private sector (private entities utilising data for commercial gain), towards threats posted by governmental national security and intelligence activities (Wilton 2017).

Despite the prevalence of definitions of privacy, a number of scholars argue that privacy is best understood as being about control, whether in relation to certain domains, such as personal information (Westin 1967) or, more generally, in the sense of controlling access to oneself (Altman 1976) or the management of social interaction (Foddy and Finighan 1980). Given that government surveillance involves, among other things, collection and use of data, including in the online context, and given that surveillance is ubiquitous and a practice over which individuals have limited control, it might be expected that individuals who are concerned about the collection and/or use of their personal information would be less likely to accept government surveillance. Thus we hypothesise:

H1: Privacy concerns regarding the collection of data will negatively influence the acceptance of surveillance

H2: Privacy concerns regarding the secondary use of data will negatively influence the acceptance of surveillance

2.2 Perceived Need for Surveillance

Although government surveillance is directed to various purposes, including prevention of crime, enforcement of revenue law and monitoring of voters, a central purpose of surveillance is national security. Indeed, one of the main arguments raised by governments to justify the implementation or increase of government surveillance is the need to protect its citizens from harm by preventing and responding to threats to national security in a more efficient manner. When large scale tragedies occur, it is often easy to suggest that lack of information prior to the event was a contributing factor. Following the terror attacks in Sydney, 2014, and Paris, 2015, the Australian Government promoted the idea that a metadata retention scheme was essential in order to protect national security, even though many questioned whether the extent of the measures was proportionate (Suzor et al. 2017). Dinev et al. (2008) found that, despite a slight decline since 9/11, there was still broad support among US citizens' for law enforcement to have even greater powers. More recently, a 2016 UK study, regarding the move to expand surveillance powers of UK intelligence organisations, found that 63% of those polled supported the expansion, with "27% claiming their opinion has changed due to recent terror activities" (Computer Business Review 2016). These results indicate that fear from ongoing attacks and/or governmental pressure is indicative of acceptance of such measures. Thus we hypothesise:

H3: Perceived need for surveillance will positively influence the acceptance of surveillance

2.3 Trust in Government, and its Management of Data

Trust in government is becoming an increasingly significant issue in many advanced democracies such as the US or UK (Hardin 2013). Many recent high-profile intrusions, such as unwarranted wire-tapping of phones (Baldwin Jr and Shaw 2006) and indiscriminate mass surveillance by government security agencies (Wilton 2017) have threatened trust in government and may influence the perception of government agencies' ability to adequately maintain data securely.

Even prior to implementation of the Australian metadata retention scheme, Australian law-enforcement agencies were already under scrutiny for accessing web histories, without a relevant warrant (Grubb 2014). In addition to high-profile leaks occurring in the United States, the leaking of confidential documents has been prominent in the Australian media in recent years (McGhee and McKinnon 2018). The loss of hundreds of highly classified documents made headlines in early 2018,

after government furniture containing a trove of classified information was sold to the public (McGhee and McKinnon 2018). Also in 2018, a high profile leak of documents appeared to reveal a proposal for the Australian Signals Directorate (ASD) to increase the scope of its monitoring to include Australian citizens (Belot 2018). These are just two recent examples of top-secret information getting into the hands of the public and the media, potentially degrading the credibility of Australia's security agencies and their ability to hold information securely.

Levels of political trust may, in turn, have implications for the extent to which citizens support government surveillance. Trüdinger and Steckermeier (2017) found a positive relationship between political trust and the support of surveillance measures in Germany. Thus we hypothesise:

H4: Trust in government will positively influence acceptance of surveillance

H5: Trust in government data management will positively influence acceptance of surveillance

2.4 Privacy Protections

Joh (2013), described a broad range of "Privacy Protests" by which individuals are able to maintain their level of privacy and reduce their digital trail, including Tor, the encryption of digital communications, the use of temporary email addresses, burner (disposable) phones, and the emphasis on using cash or prepaid debit cards. According to Wilton (2017), consumers are becoming increasingly aware of the merits of using such obfuscating tools. The difficulty in evading technological surveillance may therefore be lessening, given that all technologies can be outsmarted, given enough time, resources or ingenuity (Lyon 2003). In the context of metadata retention, for example, simply utilising a VPN, which can be obtained freely, will mean that much of the data intended to be captured will be unreadable to the ISP and that the targets of surveillance, such as criminals or terrorists, will continue to evade detection (Ockenden 2017). Choi et al. (2018) found a positive association between higher levels of privacy concerns and stronger actions taken to protect individual privacy. The US Pew Research Center showed that 34% (n = 475) of the people who were aware of the government surveillance programs exposed by former NSA contractor Edward Snowden had changed the way they protected themselves, by utilising at least one measure to shield themselves from government scrutiny (Shelton et al. 2015). That same awareness also led to 25% of individuals modifying the way they used technology "a great deal" or "somewhat" (Shelton et al. 2015). In line with these findings we hypothesise:

H6: Privacy concerns regarding the collection of data will positively influence privacy protections

H7: Privacy concerns regarding the secondary use of data will positively influence privacy protections

H8: Acceptance of surveillance will negatively influence privacy protections

3 Research Method and Design

An anonymous online survey was developed and administered using the Qualtrics platform. All participants were 18 or over and were residents of Australia. Snowball sampling was employed, with the initial distribution being conducted through the researchers own social networks, including LinkedIn and Facebook. The survey was open for data collection between April 2018 and May 2018. Human Research Ethics Committee approval was sought from our human research ethics committee prior to commencing data collection.

3.1 Survey development

The introductory section of the survey gathered general demographic information about participants including age, gender and political affiliation. The core questions to test the above hypotheses were based on validated instruments from previously published research. The dimensions considered and sources are summarized in Table 1. Survey items are available in full from the cited papers and for brevity are not replicated.

The items to measure respondents' perceptions were measured on 5 point Likert scales from 1 "Strongly Disagree" to 5 "Strongly Agree". Privacy Protections were measured using a list of ten items and respondents indicated whether or not they had adopted measures such as the use of a VPN, temporary email address or changing social media privacy settings. The overall measure of Privacy Protections was thus calculated as the sum of the responses to these ten items.

Construct	Definition	Source
Privacy Concerns of Collection	Individuals' concern that data about their personalities, background or activities is being accumulated.	Smith et al. (1996) *Collection & Improper access sub-scales*
Privacy Concerns of Secondary Use	Individuals' concern that any collected information may then be re-purposed or disclosed to other parties without authorization.	Smith et al. (1996) *Secondary use sub-scale*
Perceived Need for Surveillance	Perception that government surveillance is necessary for the protection of citizens.	Dinev et al. (2008)
Trust in Government	Individuals' level of trust in the government and legal system.	Trüdinger and Steckermeier (2017)
Trust in Government Data Management	Individuals' level of trust in the government's ability to protect data, and honesty in communicating any risks.	Siegrist et al. (2003) *Social Trust sub-scale*
Acceptance of Surveillance	Individuals' acceptance of a range of surveillance activities.	Trüdinger and Steckermeier (2017)/New items for Australian metadata retention of IP address, phone call and location data
Privacy Protections	Protective behaviours enacted to preserve online privacy.	Shelton et al. (2015)

Table 1: Survey item sources

4 Results and Analysis

Following the closure of the data collection period, a total of 129 responses had been gathered. Initial checking revealed that 29 responses were incomplete and these were not included in the data analysis. Of the 100 complete survey respondents, 55% were male and 45% female and 34% of the respondents were between the ages of 25-34 and 23% from 35-44. There were no outliers in the data, as assessed by inspection of a boxplot. Participants were also asked the political party that they felt most aligned with. Labor held the highest margin (32%), with Liberal/National affiliation ranking second (28%). When aggregated into their respective left/right position on the political spectrum, there was a 16% greater support for the left-leaning parties than for the right-leaning ones amongst participants.

Mean Privacy Concerns of Collection and Secondary Use were high (4.38 /5 and 4.76/5); most individuals strongly felt the need for protection of their privacy. The mean levels of Trust in Government Data Management were relatively low (2.38/5), with many individuals believing the government is not transparent in its acquisition of, or communication about the implications of holding private data. The mean levels of Perceived Need for Surveillance (2.90/5) and Trust in Government (2.93/5) were also slightly lower than neutral suggesting that, on average, respondents felt a relatively low need for surveillance, and were lacking trust in the government.

The average individual utilised between three and four Privacy Protections out of a possible ten. The top three Privacy Protections were "*changing your privacy settings on social media*", "*using more complex passwords*" and "*giving inaccurate or misleading information about yourself*", all of which are easily accomplished by many individuals. Over a third of the sample use a VPN, while only 10% have used Tor. There were individuals who had adopted all Privacy Protections, while some had adopted none. These findings are summarized below in Table 2.

Construct	Minimum	Maximum	Mean	SD
Privacy Concerns of Collection	2.71	5	4.38	0.56
Privacy Concerns of Secondary Use	3.5	5	4.76	0.37
Perceived Need for Surveillance	1	4.75	2.92	0.99
Trust in Government	1	5	2.93	0.83
Trust in Government Data Management	1	4.67	2.38	1.01
Acceptance of Surveillance	1.2	5	3.09	0.94
Privacy Protections	0	10	3.41	2.41

Table 2: Descriptive statistics

4.1 PLS Modelling

Since a single survey was used to collect all of the variables, we assessed the potential threat of common method variance (CMV) through a Harmon one-factor analysis. The results showed that the most variance explained by one factor was 27.9%. Therefore, CMV is unlikely to be a serious concern in this data set. The model was next tested with PLS using SmartPLS 2.0 (Ringle et al. 2005), using a bootstrap resampling method with 1000 iterations to determine the significance of the paths.

Convergent validity was confirmed by testing that all item loadings were significant and above the cut-off value of 0.50 (Hulland 1999); the composite reliabilities and Cronbach Alpha of all constructs were above 0.70 (Hulland 1999). Average variance extracted (AVE) of all constructs was above the threshold of 0.50 (Hulland 1999) with the exception of Privacy Concerns of Collection, which was marginally lower at 0.47. This was retained, as the items were drawn from a single validated scale and removal of items to increase AVE did not change the significance of paths in subsequent analysis. Discriminant validity was tested by ensuring that the square root of AVE for each construct exceeded the correlations between that construct and any other construct, and this is summarized below in Table 3. Thus, the measures of the reflective constructs demonstrated good psychometric properties.

	1	2	3	4	5	6	7
Acceptance of Surveillance	**0.73**						
Privacy Protections	-0.35	**single**					
Trust in Government Data Management	0.50	-0.39	**0.83**				
Trust in Government	0.63	-0.26	0.63	**0.81**			
Privacy Concerns of Collection	-0.35	0.22	-0.30	-0.36	**0.68**		
Privacy Concerns of Secondary Use	-0.21	0.29	-0.08	-0.16	0.44	**0.72**	
Perceived Need for Surveillance	0.71	-0.28	0.53	0.58	-0.26	-0.17	**0.87**

Table 3: Correlation between constructs and square-root of AVEs (on-diagonal)

We then examined the structural model (see Figure 1). Acceptance of Surveillance was negatively influenced by Privacy Concerns of Collection (ß = -.10, $p < .05$), and positively influenced by Perceived Need for Surveillance (ß = .50, $p < .001$) and Trust in Government (ß = .29, $p < .001$) leading us to accept H1, H3 and H4. We did not find significant support for influence of either Privacy Concerns of Secondary Use or Trust in Government Data Management thus leading us to reject H2 and H5.

In terms of protective behaviours, the results indicate that Privacy Concerns of Collection does not influence the enactment of Privacy Protections, leading us to reject H6. Interestingly, Privacy Concerns of Secondary Use does positively influence Privacy Protections (ß = .24, $p < .001$) lending support for H7. Finally, there is a strong relationship between Acceptance of Surveillance and Privacy Protections

as hypothesised in H8. These factors together explained 58.4% of variance for Acceptance of Surveillance and 17.6% of the variance in Privacy Protections.

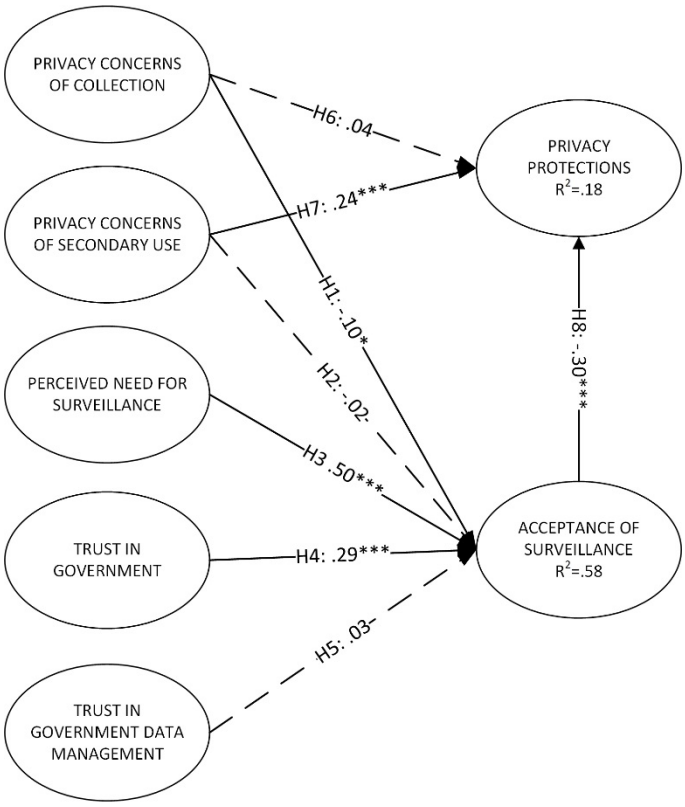

Figure 1: Calculated model

5 Discussion

The purpose of this research was to test the relationships between Privacy Concerns, the use of Privacy Protections, the Perceived Need for Surveillance, Trust in Government and Trust in Government Data Management and to identify the determinants of Acceptance of Surveillance. Five out of the eight hypotheses were supported by the results, as seen in Figure 1.

Privacy concerns about the collection of data were found to significantly influence acceptance of surveillance. This is as expected, and supports H1. Those generally concerned about their private information being gathered during online interactions, are also less accepting of government surveillance. Perhaps more interesting, is the lack of significance between privacy concerns about secondary use of data and the acceptance of surveillance: that is, concerns around secondary use did not influence acceptance. Although these are closely related concepts (i.e. it is common practice to store collected data for later repurposing), the respondents appear to have not have associated the two. One explanation for this is that individuals may hold a simplistic mental model (Thompson and McGill 2017) that surveillance is analogous to "watching" or "observing" and may not even consider the potential secondary use of this same data. However, it is also possible that some people simply do not regard being subject to surveillance as an interference with privacy. As Solove has noted (2007, 748): "When discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide." Yet this says nothing about whether those same people would be concerned about a secondary use of any data captured during surveillance. For example, a person might accept surveillance by CCTV but find it unacceptable if that footage was broadcast to a general audience as part of a television documentary. Given that the questions relating to privacy concerns about secondary use related to more general use, another possible explanation here is that people have more faith that data captured during government surveillance will not be used (or misused) for secondary purposes than they have that data captured by the private sector will not be repurposed.

Those who believed that government surveillance was needed were more likely to accept surveillance, as were those who had trust in the government: thus supporting hypotheses H3 and H4. However, there was no significant link between respondents' trust in the government's data management and the acceptance of surveillance, as had been hypothesised in H5. A possible explanation for this is that, as already discussed above, people may not consider surveillance per se as an interference with their privacy, even if they would consider the use (or misuse) of data captured during surveillance as an interference. Alternatively, people may simply fail to associate the act of surveillance with the use of data obtained during it.

Privacy concerns about the collection of data were found to not be a significant determinant of privacy protections, as had been hypothesised in H6. One possible explanation for this is that where individuals make active decisions around collection of their personal information, or feel they are making such decisions, it is possible that collection of personal information is not experienced as a loss of control, and thus not as an interference with their privacy. Another possible explanation is that while individuals are concerned about collection of their data, they nevertheless regard that collection as a "necessary evil" — the price to pay, perhaps, for receiving goods or services — and one that is not necessarily overcome by the use of privacy protections. For example, using a fake email address is not going to assist if one is purchasing goods online. Moreover, in a social media context, as Tufekci (2008) has pointed out, some people may be prepared to trade off privacy in order to reap the benefits of disclosure and publicity. This does not necessarily mean, of course, that those individuals are not concerned about the collection of their personal information, only that they may be more concerned about other things.

On the other hand, privacy concerns about secondary use of data do significantly influence the employment of privacy protections, as was hypothesised in H7. This could be for reasons similar to those explained by Brandimarte et al (2009), who found that when individuals themselves publish private information online, they believe they retain some form of control over the access and use of that information by others. Conversely, where a third party publishes that data, individuals perceive a loss of control and realise that once private information is posted online it can be accessed and used by others, even without authorisation. By analogy, and as also suggested above, it is possible that individuals possess an illusion of control in respect of information that is collected from them (because they perceive the provision of that information as an agentic act, similar to publication) but do not possess a similar perception of control in respect of the subsequent use or repurposing of that information. Moreover, as discussed above, individuals may believe that the benefits of allowing collection of their personal information outweigh the benefits of taking certain privacy protections. In terms of the secondary use of such data, however, the risks or disadvantages may be perceived to outweigh any benefits, thus influencing the utilisation of privacy protections.

Finally, as hypothesised in H8, individuals who are accepting of government surveillance measures are significantly less likely to employ privacy protections. This is consistent with Choi et al. (2018), and also provides a possible reason why the spike in searches for privacy topics (Google Trends 2018a; Google Trends 2018b) may not result in higher mean privacy protections. As longitudinal data is not available, it is however impossible to draw any inferences about trends over time.

5.1 Implications for Research and Practice

The research model employed in this study is the first to integrate these constructs into a single model which may be adopted for future research projects. Findings from this study demonstrate that individuals' perceived need for surveillance remains to be the strongest predictor of acceptance. This has practical implications, as history has shown that changes to government surveillance policies are often made as a reaction to tragic situations, and thus public acceptance of these hinges on the emotional response to these events (Reddick et al. 2015). Policy makers should exercise caution, however, as reliance on emotional responses could potentially lead to counter-productive effects if a similarly emotionally evocative story or campaign were to diminish perceived need for surveillance, leading to widespread rejection and evasion of government security policies. Arguably, this is particularly likely if such a campaign were to undermine public trust in the government, given that an individual's general trust in the government also significantly determines the acceptance of surveillance. Efforts to maintain transparency around the use of surveillance methods and techniques would potentially improve general public trust in the government, and also lead to sustained or even increased acceptance. Malhotra et al. (2004) found that when individuals are informed about surveillance policies and when clear and transparent information is provided around what is collected, feelings of control are reinforced. Consistent with control-based conceptions of privacy, therefore,

individuals who feel in control may not experience surveillance as an interference with privacy, thereby increasing acceptance of surveillance.

6 Limitations and Future Work

This research was conducted in the midst of multiple, high-profile and heavily publicised privacy and security events, including the implementation of the General Data Protection Regulation in the European Union the collection of up to 87 million Facebook users' personally identifiable information by Cambridge Analytica, discussion around forcing technological organisations to provide a "backdoor" for security agencies in Australia, and the leaking of multiple classified pieces of information by Australian security agencies. These events brought notions of privacy, security and trust into the spotlight and may have influenced the responses in the cohort.

The method of study recruitment was through a snowball sampling, with participants initially recruited through social media. By utilising more systematic methods of survey sampling and gathering information from wider areas of Australia, it would be possible to attain a larger sample of the entire Australian population, which may support the generalizability of the findings. As the scope of this research focussed only on Australia, international variations of this study, utilising this model, should be conducted. As much related work has been conducted in the US, another western culture, it is not yet possible to infer if there are cultural influences in these results. It would be valuable to conduct research in a non-western culture which may, for instance, be differentiated in terms of individualism or power-distance dimensions.

Finally, it is interesting to note that a third of respondents used a VPN. This single privacy protection is sufficient to counteract the objective of the entire metadata retention scheme in Australia, as it applies to online metadata. Therefore, it may well be that respondents are selective in their adoption of protections and opt for quality over quantity and/or that those who adopt particular privacy protections (such as use of a VPN) are generally suspicious of government surveillance. This is an area that lends itself to further investigation.

7 Conclusion

The pervasive nature of technology, the need to keep people safe and be seen to be doing so, as well as a wider awareness of "big data", has led to an expansion in government surveillance and data collection. Yet, as the Law Council of Australia has observed, it is '"unacceptable to assume the majority of Australians, who are not criminals and have the expectation to be kept safe by the state, are willing to succumb to heightened surveillance" (Bailes 2018). In order to be seen as legitimate, therefore, government surveillance needs to be widely accepted. The main contribution of this research is the identification of factors which influence acceptance of such measures. It has also served to highlight the nature and extent of protective behaviours, or privacy protections, employed and some of the drivers behind the utilisation of those protections. Ultimately, however, it must be remembered that privacy concerns are nuanced and subjective: some individuals, for example, may not perceive the practice of surveillance as an interference with their privacy at all, but would nevertheless consider the reuse and repurposing of data captured during surveillance as a privacy harm. Others may see surveillance and collection of their data as threats to their privacy, but ones they are prepared to accept as part of a broader trade off, whether for enhanced safety, personal utility or other reasons. Therefore drawing valid conclusions about privacy concerns and the drivers of those is something which can only be done if such concerns are studied at a sufficiently granular level.

8 References

Altman, I. 1976. "Privacy : A Conceptual Analysis," *Environment and behavior* (8:1), pp 7-29.

Bailes, M. 2018. "Time to Draw the Line on Government Surveillance of Citizens." Retrieved 22 July 2018, from https://indaily.com.au/opinion/2018/05/04/time-draw-line-government-surveillance-citizens/

Baldwin Jr, F.N., and Shaw, R.B. 2006. "Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law," *University of Florida Journal of Law and Public Policy* (17), pp 429-472.

Banisar, D., and Davies, S. 1999. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments," *Journal of Computer & Information Law* (18), p 1.

Belot, H. 2018. "Security Leak About Spy Agency Referred to AFP, Labor Raises Concerns with Government." from http://www.abc.net.au/news/2018-04-29/labor-blames-government-for-security-leak/9708594

Brandimarte, L., Acquisti, A., Loewenstein, G., and Babcock, L. 2009. "Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis," in: *iConference 2009*. North Carolina.

Brown, I., and Korff, D. 2009. "Terrorism and the Proportionality of Internet Surveillance," *European Journal of Criminology* (6:2), pp 119-134.

Choi, H., Park, J., and Jung, Y. 2018. "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior* (81), 2018/04/01/, pp 42-51.

Computer Business Review. 2016. "Two Thirds of Brits Support Mass Internet Surveillance Following Recent Terror Strikes." from https://www.cbronline.com/news/mobility/security/two-thirds-of-brits-support-mass-internet-surveillance-following-recent-terror-strikes-120116-4774512/

Denemark, D. 2012. "Trust, Efficacy and Opposition to Anti-Terrorism Police Power: Australia in Comparative Perspective," *Australian Journal of Political Science* (47:1), pp 91-113.

Dinev, T., and Hart, P. 2006. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10:2), pp 7-29.

Dinev, T., Hart, P., and Mullen, M.R. 2008. "Internet Privacy Concerns and Beliefs About Government Surveillance – an Empirical Investigation," *The Journal of Strategic Information Systems* (17:3), pp 214-233.

Dutton, W., Guerra, G., Zizzo, D., and Peltu, M. 2005. "The Cyber Trust Tension in E-Government: Balancing Identity, Privacy, Security," *Information Polity* (10:1-2), pp 13-23.

Foddy, W.H., and Finighan, W. 1980. "The Concept of Privacy from a Symbolic Interaction Perspective," *Journal for the Theory of Social Behaviour* (10:1), pp 1-18.

Google Trends. 2018a. "Tor: Australia." Retrieved 12/03/2018, 2018, from https://trends.google.com/trends/explore?date=2015-04-01%202015-04-30&geo=AU&q=tor

Google Trends. 2018b. "VPN: Australia." Retrieved 12/03/2018, 2018, from https://trends.google.com/trends/explore?date=2014-02-09%202018-03-12&geo=AU&q=vpn

Grubb, B. 2014. "Telstra Found Divulging Web Browsing Histories to Law-Enforcement Agencies without a Warrant." Retrieved 17/06/2018, 2018, from https://www.smh.com.au/technology/telstra-found-divulging-web-browsing-histories-to-lawenforcement-agencies-without-a-warrant-20140819-106112.html

Hardin, R. 2013. "Government without Trust," *Journal of Trust Research* (3:1), pp 32-52.

Hulland, J. 1999. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies," *Strategic management journal* (20:2), pp 195-204.

Joh, E.E. 2013. "Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion," *Arizona Law Review* (55), pp 997-1213.

Lyon, D. 2003. "Technology Vs 'Terrorism': Circuits of City Surveillance since September 11th," *International Journal of Urban and Regional Research* (27:3), pp 666-678.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp 336-355.

McGhee, A., and McKinnon, M. 2018. "The Cabinet Files." from http://www.abc.net.au/news/2018-01-31/cabinet-files-reveal-inner-government-decisions/9168442

Ockenden, W. 2017. "Metadata Retention Scheme Deadline Arrives, Digital Rights Advocates Say 'Get a VPN'." from http://www.abc.net.au/news/2017-04-13/metadata-retention-scheme-deadline-arrives/8443168

Reddick, C.G., Chatfield, A.T., and Jaramillo, P.A. 2015. "Public Opinion on National Security Agency Surveillance Programs: A Multi-Method Approach," *Government Information Quarterly* (32:2), pp 129-141.

Ringle, C.M., Wende, S., and Will, S. 2005. "Smartpls 2.0 (M3)." Hamburg.

Robert, A. 2015. "Outcry over French Intelligence Bill." Retrieved 13/03/2018, 2018, from http://www.euractiv.com/sections/infosociety/outcry-over-french-intelligence-bill-313779

Shelton, M., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A., and Page, D. 2015. "Americans' Privacy Strategies Post-Snowden," Pew Research Centre.

Siegrist, M., Earle, T.C., and Gutscher, H. 2003. "Test of a Trust and Confidence Model in the Applied Context of Electromagnetic Field (EMF) Risks," *Risk Analysis: An International Journal* (23:4), pp 705-716.

Smith, H., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp 989-1016.

Smith, H., Milberg, S., and Burke, S. 1996. "Information Privacy: Measuring Individual's Concerns About Organizational Practices," *MIS Quarterly* (20:2), p 167.

Suzor, N.P., Pappalardo, K.M., and McIntosh, N. 2017. "The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny," *Internet Policy Review* (6:1), pp 1-16.

Thierer, A. 2013. "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law & Public Policy* (36), pp 409-455.

Thompson, N., and McGill, T. 2017. "Mining the Mind–Applying Quantitative Techniques to Mental Models of Security," *Australasian Conference on Information Systems 2017 (ACIS 2017)*.

Trüdinger, E.-M., and Steckermeier, L.C. 2017. "Trusting and Controlling? Political Trust, Information and Acceptance of Surveillance Policies: The Case of Germany," *Government Information Quarterly* (34:3), pp 421-433.

Tufekci, Z. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society* (28:1), pp 20-36.

Westin, A.F. 1967. *Privacy and Freedom*. London: The Bodley Head Ltd.

Whitman, J.Q. 2003. "The Two Western Cultures of Privacy: Dignity Versus Liberty," *Yale Law Journal* (113), pp 1151-1222.

Wilton, R. 2017. "After Snowden – the Evolving Landscape of Privacy and Technology," *Journal of Information, Communication and Ethics in Society* (15:3), pp 328-335.