# Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance

**Nik Thompson** (Corresponding Author)
School of Management
Curtin University
Perth, Australia
Email: nik.thompson@curtin.edu.au
Tel +61-8-92667198

**Tanya McGill**
Discipline of Information Technology. Mathematics and Statistics
Murdoch University
Perth, Western Australia
Email: t.mcgill@murdoch.edu.au
Tel +61-8-93602798

**Anna Bunn**
Curtin Law School
Curtin University
Perth, Australia
Email: a.bunn@curtin.edu.au
Tel +61-8-92667379

**Rukshan Alexander**
Department of Economics and Management
Vavuniya Campus, University of Jaffna
Vavuniya, Sri Lanka
Email: a.rukshan@vau.jfn.ac.lk

## Abstract

Though there is a tension between citizens' privacy concerns and their acceptance of government surveillance, there is little systematic research in this space, and less still in a cross cultural context. We address the research gap by modeling the factors that drive public acceptance of government surveillance, and by exploring the influence of national culture. The research involved an online survey of 242 Australian and Sri Lankan residents. Data was analyzed using PLS, revealing that privacy concerns around initial collection of citizens' data influenced levels of acceptance of surveillance in Australia but not Sri Lanka, whereas concerns about secondary use of data did not influence levels of acceptance in either country. These findings suggest that respondents conflate surveillance with the collection of data and may not consider subsequent secondary use. We also investigate cultural differences, finding that societal collectivism and power distance significantly affect the strength of the relationships between privacy concerns and acceptance of surveillance, on the one hand, and adoption of privacy protections, on the other. Our research also considers the role of trust in government, and perceived need for surveillance. Findings are discussed with their implications for theory and practice.


## Introduction

In recent years, citizens in many jurisdictions have found themselves subject to increasing levels of routine government surveillance (Denemark, 2012) which takes many forms. While there is debate about exactly what constitutes surveillance and when it occurs (Bernal, 2016; Marx, 2015) it is essentially concerned with the strategic collection of information of data about citizens (Trüdinger & Steckermeier, 2017). Collection of data can occur in offline and online environments, and government surveillance strategies may involve direct collection of citizens' personal information or may require data to be collected and provided by third parties. As an example of the latter, a recently implemented metadata retention regime in Australia mandates that communications service providers log their customers' location data and online activities for two years (Parliament of the Commonwealth of Australia, 2015).

Online surveillance of citizens (as with offline surveillance) is generally justified for its role in the prosecution and prevention of crime and the prevention of activities that threaten national security (Parliament of the Commonwealth of Australia, 2015). Nevertheless, members of the public are often opposed to such measures and may seek ways to avoid being monitored (Joh, 2013). There is some anecdotal evidence that this is the case. For example, internet searches for privacy protections such as virtual private networks (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, 2018b).

Public acceptance of surveillance is influenced by various factors, including privacy concerns (Dinev & Hart, 2006; Dinev, Hart, & Mullen, 2008), the perceived need for surveillance (Brown & Korff, 2009; Dutton, Guerra, Zizzo, & Peltu, 2005), and trust in the government (Trüdinger & Steckermeier, 2017). Much research as to the factors that influence public acceptance of government surveillance has been conducted in the US context; however, revelations about Edward Snowden's leaks have led to increased interest in the government surveillance perceptions of citizens in other countries (e.g., Adams Andrew, 2017a, 2017b; Murata, 2017a; Murata, 2017b). There has also been little research into whether the use of privacy protections is influenced by acceptance of government surveillance and privacy concerns and to what extent national culture plays a role in influencing public acceptance of surveillance or the adoption of privacy protections. The latter question is particularly important given culture is one factor that informs public opinion about surveillance (Hallinan & Friedewald, 2012). Moreover, an increasing number of privacy scholars advocate for a more contextual approach to information privacy (Wu, Vitak, & Zimmer, 2019) and surveillance clearly implicates privacy, although is not necessarily in opposition to it (Marx, 2015).

Our research sought to discover some of the factors that influence public acceptance of government surveillance in the online environment, as well as factors that influence the uptake of privacy protections. References to "government surveillance" in the context of our model, therefore, are references to online government surveillance. Our central research questions are twofold. First: What are the determinants of acceptance of government surveillance and the use of privacy protections? Second: Does national culture influence the

strength of any relationship between privacy concerns, acceptance of surveillance and the adoption of privacy protections?

We address the research gap by developing a model that considers factors previously found to drive public acceptance of government surveillance, as well as factors thought to influence the adoption of privacy protections. We then empirically evaluate this model by gathering survey data from 242 residents of Australia and Sri Lanka and analyzing 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.

## Theoretical Framework and Research Hypotheses

While state surveillance of citizens has increased ─ due, in part, to the opportunities provided by new technologies (Reddick, Chatfield, & Jaramillo, 2015) ─ public views on that surveillance are mixed (Dinev et al., 2008; Parliamentary Joint Committee on Intelligence and Security, 2015; Rainie & Madden, 2015; Robert, 2015) and may not be well understood (Reddick et al., 2015). Much of the research into factors that influence public acceptance of surveillance has been conducted in the US, yet differences in national legal frameworks and cultural norms, among other things, are likely to impact upon the extent to which citizens accept such surveillance and the factors that influence that acceptance. Moreover, it is possible that the national context may influence the extent to which individuals adopt privacy protective measures, as well as the type of measures they take. For example, Adams Andrew (2017b) found that Spanish citizens are relatively accepting of government surveillance if they perceive a benefit to society. However, Wu et al. (2019) suggest that individuals in authoritarian regimes may face greater privacy risks vis-à-vis those in authority. It is possible, therefore, that those individuals would be more likely to adopt protective measures.

Our study is also motivated by current events in Australia and Sri Lanka. Following the introduction in 2015 of a national metadata retention regime, at the end of 2018 Australia passed so-called “encryption laws”. These encryption laws introduced measures that compel communications providers to assist law enforcement and security agencies to deal with the challenges posed by “ubiquitous encryption” (Parliament of the Commonwealth of Australia, 2018). In 2018, following an outbreak of communal violence in Sri Lanka (Safi & Perera,

2018) the President of Sri Lanka revealed plans for "implementing the necessary monitoring and surveillance methods to ensure the public safety" (Sri Lanka Government, 2018).

Hallinan and Friedwald (2012) identify two reasons why public perceptions of government surveillance practices are important: firstly, because public opinion is a "shaping factor…in the development of surveillance technologies and surveillance infrastructures" (p.2); and secondly because in democratic societies public opinion should shape public policy. Similarly, 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). Public acceptance of surveillance may be important for other reasons, however a lack of public support for surveillance measures could "undermine government efforts to increase protection for the public" (Dinev et al., 2008, p. 227). In this research, we study several potential determinants of public acceptance of surveillance, including privacy concerns, perceived need for surveillance, and trust in government. We also investigate whether national culture plays a role. 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, Earle, & Gutscher, 2003; Trüdinger & Steckermeier, 2017). Figure 1 shows the proposed research model. The justifications for the inclusion of these constructs and the associated hypotheses are discussed in the following sections.

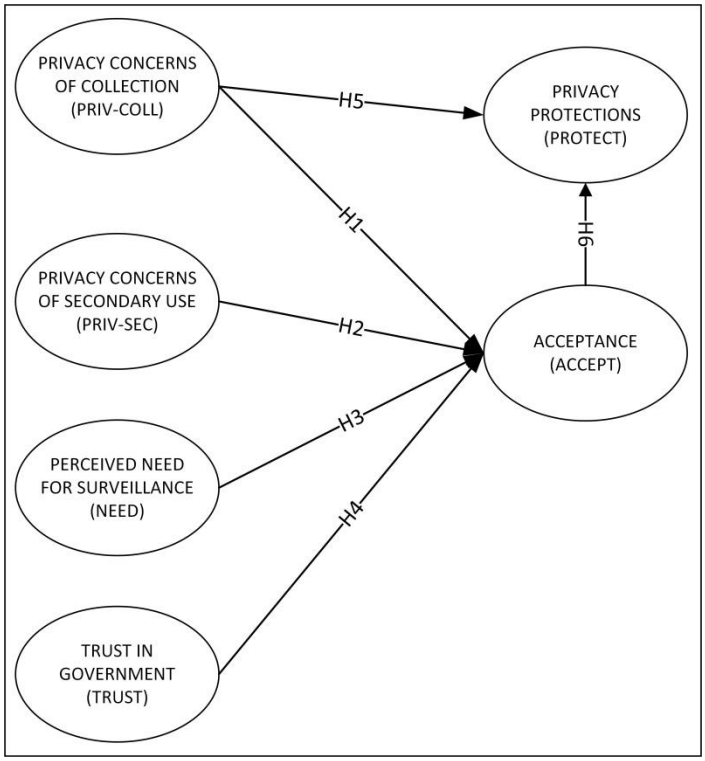


Fig 1: Research model

## National culture

Stemming from the work of Kluckhohn (1962 ), scholars have proposed models to explain and understand how members of a society share beliefs and values. Most prominent among these is Hofstede's model (2011) which describes a national culture in terms of six dimensions; in this model, culture is defined as "the collective programming of the mind that distinguishes the members of one group or category of people from others" (p.3). Although every collective is comprised of individuals, in aggregate the members of a collective often exhibit similar patterns along the six dimensions. Differences in cultural dimensions are associated with differences in privacy concerns in some domains. For example, high power distance has been shown to be related to higher levels of concerns over social network services (SNS) privacy, and higher levels of individualism have been found to be related to lower levels of privacy concerns (Cecere, Le Guel, & Soulié, 2015). Differences in these dimensions may also have implications for how members of a society accept government surveillance or how they enact measures to protect their privacy. Given their relevance to privacy and surveillance, and the fact that there are marked differences between Australia and

Sri Lanka in respect of these two dimensions (Hofstede Insights, 2019), we focus on the dimensions of individualism/collectivism and power distance.

Power distance refers to the extent to which members of a society accept that power distribution is unequal. It suggests that inequality in society is endorsed not only by leaders but also by the mainstream. Put simply, members of a high power distance culture expect to be told what to do. With a relatively high score of 80 (out of 120), Sri Lanka can be considered to be towards the higher side in terms of power distance. Australia ranks far lower, scoring 36 in this dimension (Hofstede Insights, 2019).

Individualism/collectivism refers to the degree to which members of a society are integrated into groups. This relates to whether a person holds a self-image of "I" versus a self-image of "we". Individualist societies have loose ties, and everyone is expected to look after themselves. On the other hand, collectivist societies emphasize the interests of the group in their daily life. With a low score of 35, Sri Lanka is considered to be a collectivist society. Australia, in contrast, has a high score of 90 indicating that it is an individualist society (Hofstede Insights, 2019).

The impact of the two dimensions of power distance and individualism on the constructs included in the research model is revisited, with specific hypotheses, below.

## Determinants of Acceptance of Government Surveillance

### Privacy concerns

Privacy has been described as an "evanescent concept" (Gormley, 1992, p. 1336) and one that is notoriously difficult to define (Smith, Dinev, & Xu, 2011). The definitional problem arises in part because privacy is likely to be differentially experienced depending on context: geographical, cultural, temporal and otherwise (e.g. Thierer, 2013; Whitman, 2003). Various and to some extent overlapping domains of privacy have been identified including information privacy, territorial privacy, bodily privacy and privacy of communications (Banisar & Davies, 1999). In terms of personal information, Dinev, Hart and Mullen (2008) report that 94% of Americans polled were worried (or very worried) about the misuse of that information. However, whereas threats to information privacy have traditionally been perceived as originating primarily from the private sector (private entities utilizing data for

commercial gain), increasingly such concerns are directed towards governmental national security and intelligence activities (Wilton, 2017).

While privacy may elude a unitary definition, various scholars have argued that it should be understood in terms of control. Westin (1967; p.10), for example, defined privacy as "the right of the individual to decide what information about himself should be communicated to others and under what condition". Although Westin's definition may be contestable in contemporary times (Wu et al., 2019), the importance of control over personal information is recognized in the General Data Protection Regulation (European Parliament, 2016, Recital 7) and control over personal information is clearly important to individuals (European Commission, 2016; Hallinan & Friedewald, 2012). Given that government surveillance involves collection and use of data 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 or use of their personal information would be less likely to accept government surveillance. Thus we hypothesize:

***H1****: Privacy concerns regarding the collection of data will negatively influence the acceptance of surveillance in both cultures.*

***H2****: Privacy concerns regarding the secondary use of data will negatively influence the acceptance of surveillance in both cultures.*

## Privacy Concerns: Cultural Influences

Those in high power distance cultures are accustomed to an unequal distribution of authority. Hence, they are more likely to tolerate governmental interferences with privacy than those in low power distance cultures (Bandyopadhyay, 2009). In the consumer space, Wu, Huang, Yen, and Popova (2012) showed that the relationship between privacy concerns and acceptance of information collection is moderated by power distance. Milberg, Burke, Smith, and Kallman (1995) explain that individuals in countries high on the power distance index have lower levels of interpersonal trust. As a consequence, individuals in those countries may not only accept but even desire greater government involvement, which is seen as a means to protect them. Moreover, as those from high power distance cultures are used to a hierarchical social structure they may be more accepting of information gathering from those in a position of authority (Cao & Everard, 2008) and the influence of any personal concerns may be weaker. Thus, we hypothesize:

***H1$_a$**: The negative relationship between privacy concerns of collection and acceptance of surveillance will be weaker in cultures higher on power distance.*

***H2$_a$**: The negative relationship between privacy concerns of secondary use and acceptance of surveillance will be weaker in cultures higher on power distance*

## Perceived need for surveillance

Government surveillance has various objectives, including prevention of crime, enforcement of revenue law, and monitoring of voters (Bennett, 2015). However, a central purpose of surveillance is national security (Parliament of the Commonwealth of Australia, 2015; Reddick, Chatfield, & Jaramillo, 2015). Indeed, one of the main arguments raised by governments to justify the implementation of or increase in 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 (Allison, 2017; Porter, 2018). When large scale tragedies occur, lack of intelligence prior to the event is often cited as a contributing factor (Smith & Ferndando, 2019). Accordingly, an increase in government surveillance powers may be easier to justify in the wake of such tragedies. Following the terror attacks in Sydney, 2014, and Paris, 2015, for example, the Australian Government promoted the idea that a metadata retention scheme was essential to protect national security, even though many questioned whether the extent of the measures was proportionate (Suzor, Pappalardo, & McIntosh, 2017). Moreover, public support for the extension of government surveillance powers might be galvanized by such events. Dinev et al. (2008) found that there was still broad support among US citizens for law enforcement to have even greater powers, albeit that the levels of support had declined slightly from those seen in the immediate aftermath of 9/11. More recently, a 2016 UK study regarding the move to expand surveillance powers of UK intelligence organizations found that 63% of those polled supported the expansion, with 27% claiming their opinion had "changed due to recent terror activities" (Computer Business Review, 2016). Thus, we hypothesize:

***H3**: Perceived need for surveillance will positively influence the acceptance of surveillance in both cultures.*

## Trust in government

Within many advanced democracies, such as the US and UK, trust in government is an increasingly significant issue (Hardin, 2013; Intawan & Nicholson, 2018). Trust in government can be undermined for different reasons including, but not of course limited to, the extent to which governments manage information. In this regard, high-profile government intrusions into private lives, such as through unwarranted wire-tapping of phones (Baldwin & Shaw, 2006) and indiscriminate mass surveillance by government security agencies (Wilton, 2017) have threatened trust in government and may influence perceptions of the ability of government agencies to adequately maintain data securely. However, whilst a significant proportion of US citizens express a lack of trust in government, Intawan and Nicholson (2018), report that the majority of US citizens maintain a positive implicit trust in government, whilst exhibiting a negative explicit trust.

In addition to high-profile leaks occurring in the US, it has been recently reported that a database storing sensitive biometric data and other personal information and integrated with a system used by numerous countries and government services, including the UK Metropolitan Police Force, was easily accessible to third parties and "largely unsecured" (Jain, 2019). In Australia, the leaking of confidential documents has been prominent in the media in recent years (McGhee & McKinnon, 2018) and even prior to the implementation of the Australian metadata retention scheme law-enforcement agencies were under scrutiny for accessing web histories, without a relevant warrant (Grubb, 2014).

Aside from the extent to which people trust the government to manage and secure information, general levels of trust in the government, or political trust may have a bearing on the extent to which citizens support government surveillance. Indeed, Davis and Silver (2004) found that the more trust citizens have in their government the more willing they are to accept government security measures. Likewise, Trüdinger and Steckermeier (2017) found a positive relationship between political trust and the support of surveillance measures in Germany. Thus, we hypothesize:

***H4****: Trust in government will positively influence acceptance of surveillance in both cultures.*

## Privacy protections

Various means are open to individuals to reduce their digital trails and avoid surveillance. These include the use of Tor, burner (disposable) phones, temporary email addresses and cash in preference to debit cards, as well through the encryption of digital communications (Joh, 2013). Wilton (2017) observed that consumers are becoming increasingly aware of the merits of using such obfuscating tools, and levels of use of privacy protections have increased in the US since the Snowden leaks (Rainie & Madden, 2015). According to Lyon (2003, p.675) "human beings are more flexible and imaginative than technologies" and thus possess the capacity to outsmart those technologies and, by so doing, evade surveillance. In the context of metadata retention, for example, simply utilizing a VPN, which can be obtained freely, will mean that much of the data intended to be captured will be unreadable to the Internet Service Provider (ISP). Use of such measures need not be an indication of criminality: it might simply represent a protest against the surveillance itself (Joh, 2013). However, the use of evasion tools can allow the intended targets of surveillance, such as criminals or terrorists, to evade detection (Ockenden, 2017).

Researchers have found a positive association between higher levels of privacy concerns and greater efforts to protect individual privacy (Choi, Park, and Jung (2018). Similarly, research conducted by Pew Research Center found that 34% ($n$ = 475) of those who were aware of the government surveillance programs exposed by former National Security Agency contractor Edward Snowden had changed the way they protected themselves, by utilizing at least one measure to shield themselves from government scrutiny (Shelton et al., 2015). For the same reason, 25% of individuals modified the way they used technology "a great deal" or "somewhat" (Shelton et al., 2015). In line with these findings we hypothesize:

***H5****: Privacy concerns regarding the collection of data will positively influence use of privacy protections.*

***H6****: Acceptance of surveillance will negatively influence use of privacy protections.*

### Privacy Protections: Cultural Influences

Members of a collectivist society attempt to fit in with others and place more emphasis on groups (Markus & Kitayama, 1991). Therefore, to fit in with the shared norms and protect each other's privacy, they may be more likely to employ privacy protections. This is because

members are more concerned about the privacy harms that may be experienced by their collective (Posey et al. 2010). Trepte et al. (2017) examined the well-known privacy calculus framework in the context of culture, confirming that those with higher levels of collectivism did place a greater emphasis on privacy protections, presumably in order to safeguard their collective. Dinev, Goo, Hu, and Nam (2009) also showed that culture moderates the intentions to use protective technology; a finding which is associated with the cultural influence on perceptions about privacy (Milberg, Smith, & Burke, 2000). Consistent with Altman's (1977) position that different cultures have different mechanisms for regulating their behavior and interactions, we hypothesize that:

***H5$_a$**: The positive relationship between privacy concerns and privacy protections will be stronger in collectivist cultures.*

***H6$_a$**: The negative relationship between acceptance of surveillance and privacy protections will be weaker in collectivist cultures.*

# Research Method

An anonymous online survey was developed and administered using the Qualtrics platform. All participants were 18 or over and were residents of Australia and Sri Lanka. Australia was selected as a relatively low power distance and high individualism country, and Sri Lanka was selected as a relatively high power distance and high collectivism country. In Australia the language used in the survey instrument was English. For Sri Lanka, the survey was translated from English into Tamil and Sinhalese by native speakers. Data analysis was conducted using SPSS 25 and Smart PLS 2.0 packages for statistical and PLS structural equation modelling.

The introductory section of the survey gathered general demographic information about participants including age and gender. The second section asked about the privacy-related perceptions and behaviors of participants. Where possible, the items to measure the constructs in the model were based on validated instruments from previously published research. Table 1 provides definitions of the constructs in the model and summarizes the sources of the items used to measure them.

The items to assess respondents' perceptions were measured on 5 point Likert scales from 1 "Strongly Disagree" to 5 "Strongly Agree". The trust items consider levels of trust in different government agencies, therefore this construct is a composite of multiple measures

and was modelled formatively (MacCallum & Browne, 1993). Privacy protections were assessed by asking respondents to indicate which of a list of ten privacy protective measures, they had adopted. An overall measure of privacy protections was calculated for each participant as the total number of privacy measures that they had adopted. All other constructs were modelled reflectively.

Table 1: Survey Items

| **Construct** | **Definition** | **Source + (No. of items)** |
|---|---|---|
| Privacy Concerns of Collection (PRIV-COLL) | Individuals' concerns that data about their personalities, background or activities are being accumulated. | Smith, Milberg, and Burke (1996) (4) |
| Privacy Concerns of Secondary Use (PRIV-SEC) | Individuals' concerns that any collected information may then be re-purposed or disclosed to other parties without authorization. | Smith et al. (1996) (4) |
| Perceived Need for Surveillance (NEED) | Perception that government surveillance is necessary for the protection of citizens. | Dinev et al. (2008) (4) |
| Trust in Government (TRUST) | Individuals' level of trust in the government and legal system. | Trüdinger and Steckermeier (2017) (3) |
| Acceptance (ACCEPT) | Individuals' acceptance of modern online surveillance activities. | Items based on types of metadata that are the subject of government retention schemes (e.g. IP address, phone call and location data) (5) |
| Privacy Protections (PROTECT) | Behaviors enacted to preserve online privacy. | Shelton et al. (2015) (10) |

Initial survey development was conducted in English, as the source items for the constructs had been previously published in English. The items to measure each construct were first pre-tested by two academics to establish content validity, and the full questionnaire was then pilot tested with five respondents from Australia. Next, the survey was professionally translated to Tamil and Sinhalese, followed by a pre-test by an academic fluent in these languages. After the pre-test, the full questionnaire was then pilot tested with ten respondents from Sri Lanka (five for each survey version). In response to pilot testing feedback, minor changes were made to the wording and to streamline the interface.

A convenience sample was recruited through snowball sampling, with the initial distribution being conducted through social networks, including LinkedIn and Facebook. The survey was open for data collection from mid-2018 to early 2019. Human Research Ethics Committee approval was obtained from our human research ethics committee before commencing data collection.

## Results and Analysis

Following the closure of the data collection, incomplete responses were screened, leaving a total sample of 242 for data analysis - 100 from Australia and 142 from Sri Lanka (comprised of 76 Sinhalese Language and 66 Tamil language responses). There was even gender balance, with 45% and 47% female respondents in Australia and Sri Lanka respectively. The most common age grouping was 25-34 years (34% AU, 47% SL).

Privacy concerns for collection (4.38-4.48) and secondary use (4.61-4.76) were generally high in both countries; most individuals strongly felt the need for protection of their privacy. The mean levels of trust (2.88-2.95) were slightly lower than neutral suggesting that, on average, respondents were lacking trust in their government. Perceived need for surveillance (2.92-4.17) was generally above neutral suggesting that respondents believe that there are some necessary elements to surveillance.

The average individual utilized between three and four privacy protections out of a possible ten. The top two protections were the same in both countries: "*changing your privacy settings on social media*" and "*using more complex passwords*" both of which are easily accomplished by many individuals. Around a third of the sample used a VPN, while only 5-10% had used Tor. Some individuals had adopted all of the individual privacy protections, while some had adopted none. These findings are summarized below in Table 2.

Table 2: Descriptive statistics

| Construct | Minimum | Maximum | Mean | SD | CR |
|---|---|---|---|---|---|
| **Australia** | | | | | |
| PRIV-COLL | 2.75 | 5 | 4.48 | 0.53 | 0.80 |
| PRIV-SEC | 3.5 | 5 | 4.76 | 0.37 | 0.75 |
| NEED | 1 | 4.75 | 2.92 | 0.99 | 0.93 |
| TRUST | 1 | 5 | 2.95 | 0.89 | * |
| ACCEPT | 1 | 5 | 2.70 | 1.25 | 0.96 |
| PROTECT | 0 | 10 | 3.41 | 0.24 | * |
| **Sri Lanka** | | | | | |
| PRIV-COLL | 2.25 | 5 | 4.38 | 0.55 | 0.74 |
| PRIV-SEC | 2.75 | 5 | 4.61 | 0.51 | 0.46 |
| NEED | 1.75 | 5 | 4.17 | 0.69 | 0.82 |
| TRUST | 1 | 5 | 2.88 | 0.86 | * |
| ACCEPT | 1 | 5 | 3.65 | 0.90 | 0.89 |
| PROTECT | 0 | 10 | 3.08 | 2.16 | * |

*Note: Although the items to measure the constructs were measured using ordinal scales, reporting of mean and SD is appropriate (Norman, 2010).*

** CR only applicable for reflective constructs.*

Since a single questionnaire was used to measure 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 36.3% in the Australian data set and 18.9% in the Sri Lankan data set. Therefore, CMV is unlikely to be a serious concern. The model was next tested with PLS, using a bootstrap resampling method with 2000 iterations to determine the significance of the paths.

Internal consistency reliability was evaluated using composite reliability (CR) as recommended by Hair, Hult, Ringle, and Sarstedt (2016). All but one CR value exceeded the suggested threshold of 0.6 for exploratory research (see Table 2). Convergent validity was evaluated by testing that all item loadings were significant and through average variance extracted (AVE) – a measure of the amount of variance in the construct relative to measurement error. Most AVE's were above or close to 0.5. According to Fornell and Larcker (1981), AVE below 0.5 is acceptable if the CR is above 0.6. This criterion was met for all constructs except PRIV-SEC and only in the Sri Lankan group. Thus, we can state that

convergent validity was established for the overall model, though the results for PRIV-SEC in the Sri Lankan group must be interpreted in light of the construct's convergent validity results. 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 in Table 3. Thus, the measures of the reflective constructs demonstrated acceptable psychometric properties.

Table 3: Construct correlations and square root of AVE on diagonal

| | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| **Australia** | | | | | | |
| ACCEPT | 0.92 | | | | | |
| PROTECT | -0.27 | 1.00 | | | | |
| TRUST | 0.55 | -0.27 | 1.00 | | | |
| PRIV-COLL | -0.31 | 0.19 | -0.30 | 0.71 | | |
| PRIV-SEC | -0.19 | 0.27 | -0.14 | 0.43 | 0.66 | |
| NEED | 0.65 | -0.28 | 0.61 | -0.22 | -0.18 | 0.87 |
| **Sri Lanka** | | | | | | |
| ACCEPT | 0.78 | | | | | |
| PROTECT | 0.07 | 1.00 | | | | |
| TRUST | 0.16 | -0.01 | 1.00 | | | |
| PRIV-COLL | 0.04 | 0.30 | -0.14 | 0.66 | | |
| PRIV-SEC | -0.08 | 0.07 | 0.00 | 0.24 | 0.56 | |
| NEED | 0.26 | 0.24 | 0.07 | 0.20 | 0.26 | 0.74 |

We then examined the structural model (see Figure 2). ACCEPT was negatively influenced by PRIV-COLL (ß = -.14, $p < .001$) for Australians, but not for Sri Lankans (ß = .04, $p = .34$) giving partial support for H1. ACCEPT was not influenced by PRIV-SEC in either culture (AU ß = -.01, $p = .39$; SL ß = -.16, $p = .17$) leading us to reject H2. ACCEPT was positively

influenced by NEED (AU ß = .50, p < .001; SL ß = .28, p < .001) and TRUST (ß = .21, p < .001, ß = .14, p < .05) in both cultures leading us to accept H3 and H4.

PROTECT was positively influenced by PRIV-COLL in both cultures (AU ß = .12, p < .05; SL ß = .29, p < .001) supporting H5. PROTECT was negatively influenced by ACCEPT, but only in Australia (ß = -.23, p < .001; ß = .06, p = .24) lending partial support for H6.

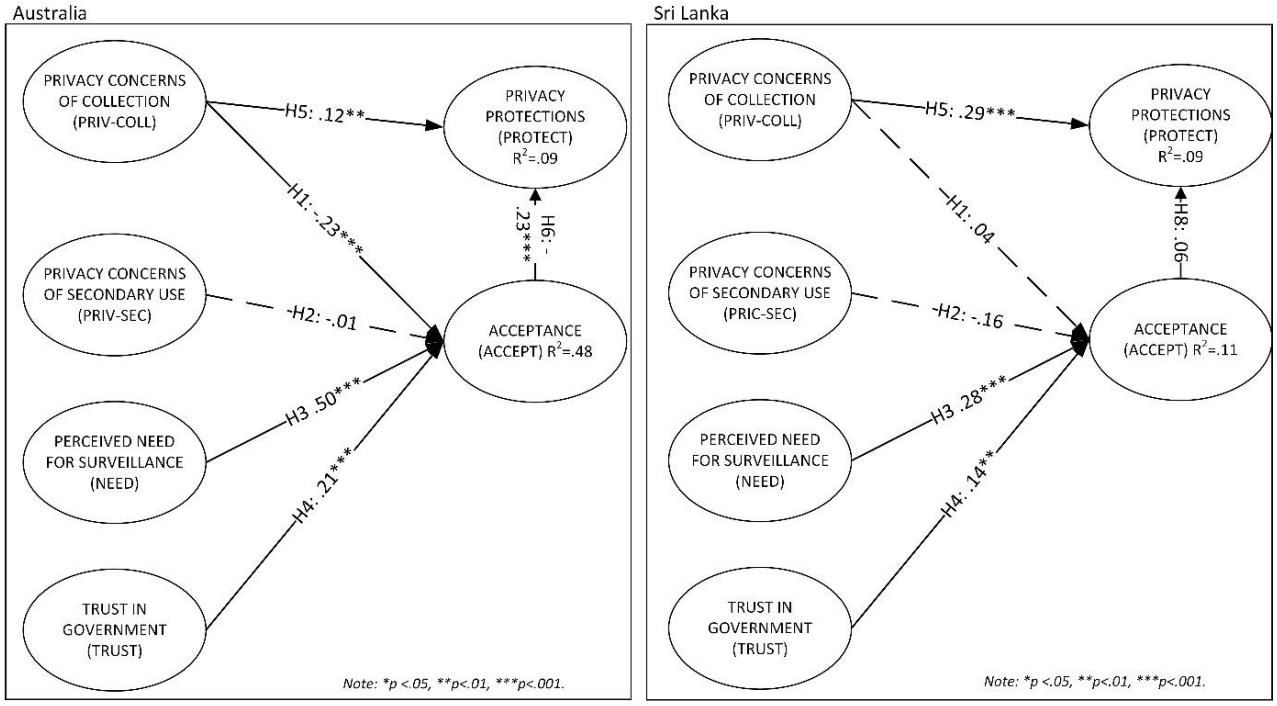


Fig 2: Structural model results

There was, however, a difference in the ability of the model to explain the variance in acceptance of government surveillance in the two cultures. The $R^2$ for ACCEPT was 0.48 for the Australians, but only 0.11 for the Sri Lankans. This suggests that other possible determinants of acceptance of government surveillance need to be considered.

Next, we assessed the role of cultural differences using the formula of Keil et al. (2000) (see Table 4). The effect of PRIV-COLL on ACCEPT was significantly weaker for Sri Lankans (with a higher power distance) lending support for $H1_a$. The relationship between PRIV-SEC use and ACCEPT was non-significant in both cultures so $H2_a$ could not be meaningfully evaluated and is not supported.

In terms of protective behaviors, the results indicate that PRIV-COLL more strongly influenced PROTECT for Sri Lankans (a collectivist society), leading us to accept $H5_a$. Finally, the negative relationship between ACCEPT and PROTECT is weaker in Sri Lanka as hypothesized in $H6_a$, providing support for the hypothesis. Table 5 summarizes the results of all of the hypothesis testing.

Table 4: Path coefficient comparison

| | **Australia** | | **Sri Lanka** | | |
|---|---|---|---|---|---|
| | ß | S.E. | ß | S.E. | P |
| PRIV-COLL→ACCEPT (H1a) | -0.14 | 0.03 | 0.04 | 0.07 | p<.001 |
| PRIV-SEC→ACCEPT (H2a) | -0.01 | 0.03 | -0.16 | 0.12 | NA |
| PRIV-COLL→PROTECT (H5a) | 0.12 | 0.04 | 0.29 | 0.04 | p<.001 |
| ACCEPT→PROTECT (H6a) | -0.23 | 0.05 | 0.06 | 0.05 | p<.001 |

Table 5: Summary of hypothesis testing

| **Hypothesis** | **Result** |
|---|---|
| **H1**: Privacy concerns regarding the collection of data will negatively influence the acceptance of surveillance in both cultures | Partially supported |
| **$H1_a$**: The negative relationship between privacy concerns of collection and acceptance of surveillance will be weaker in cultures higher on power distance. | Supported |
| **H2**: Privacy concerns regarding the secondary use of data will negatively influence the acceptance of surveillance in both cultures. | Not supported |
| **$H2_a$**: The negative relationship between privacy concerns of secondary use and acceptance of surveillance will be weaker in cultures higher on power distance. | Not supported |
| **H3**: Perceived need for surveillance will positively influence the acceptance of surveillance in both cultures. | Supported |
| **H4**: Trust in government will positively influence acceptance of surveillance in both cultures. | Supported |
| **H5**: Privacy concerns regarding the collection of data will positively influence use of privacy protections. | Supported |
| **$H5_a$**: The positive relationship between privacy concerns and privacy protections will be stronger in collectivist cultures. | Supported |
| **H6**: Acceptance of surveillance will negatively influence use of privacy protections. | Partially supported |

| | |
|---|---|
| **H6$_a$**: The negative relationship between acceptance of surveillance and privacy protections will be weaker in collectivist cultures. | Supported |

## Discussion

One objective of this research was to investigate the determinants of acceptance of government surveillance. Privacy concerns about the collection of data were found to significantly influence acceptance of surveillance by Australian residents. However, such concerns did not influence acceptance of surveillance on the part of Sri Lankans. Thus, H1 was only partially supported.

Surprisingly, privacy concerns about secondary use of collected data appeared to play even less of a role in determining acceptance of surveillance. It did not influence acceptance in either group, leading us to reject H2. Although collection of data and secondary use of it are closely related concepts (i.e. it is common practice to store collected data for later repurposing), participants appear not to have associated the two. One explanation for this is that individuals may hold a simplistic mental model (Thompson & McGill, 2017) that surveillance is analogous to "watching" or "observing" and may not even consider the potential secondary use of this same data.

The research also considers whether the influence of privacy concerns on acceptance of surveillance is affected by national culture. Hypotheses $1_a$-$2_a$ proposed that the strength of the relationships between privacy concerns and acceptance would vary due to differences in power distance in the two national cultures. $H1_a$ was supported as the relationship was stronger in the Australian group, that is, the country with lower power distance. As hypothesized, those from higher power distance countries appear to be more accepting of those in positions of authority collecting information (Cao & Everard, 2008), thus weakening the influence that privacy concerns otherwise have on acceptance of surveillance. As H2 was not supported for either group, it was not possible to meaningfully compare the difference between groups and thus $H2_a$ was not supported.

In both cultures, 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.

Privacy concerns about the collection of data were found to be a significant determinant of use of privacy protections in both cultures, as hypothesized in H5 and consistent with the findings of Choi et al. (2018). This relationship was stronger for the Sri Lankans (a collectivist culture) as hypothesized in $H5_a$, reflecting a stronger desire to protect the privacy of their collective. The stronger relationship might also be explained by the fact that countries higher on the power index, generally exhibit lower levels of interpersonal trust (Milberg et al. (1995)). However, acceptance of surveillance only had a negative influence on the use of privacy protections in the Australian group, thus H6 was only partially supported. Consistent with the partial support for H6, $H6_a$ was supported as the negative relationship between acceptance and privacy protection was stronger in the more individualistic culture (Australian). In addition to our proposed cultural differences, Dinev et al. (2009) note that differences in levels of knowledge about how to take protective action may also play a role in differences in technology related protective behavior between countries.

## Implications for research and practice

The research model employed in this study is the first to integrate these constructs into a single model that may be adopted for future research. Findings from this study demonstrate that individuals' perceived need for surveillance and trust in government are important predictors of acceptance of surveillance. 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). Policymakers 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 significantly determines the acceptance of surveillance. At the time of writing, an example of this is playing out on the streets of Hong Kong where protestors have demanded the removal of public infrastructure over concerns that it is being used for surveillance by Chinese authorities (Associated Press, 2019). 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, Kim, and Agarwal (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 interference with privacy, thereby increasing acceptance of surveillance.

The cultural dimensions discussed are applicable at not only the national level but also at organizational and occupational levels (Helmreich & Merritt, 2017). Thus our findings have practical workplace implications since organizational cultures are acquired during the course of work, and may be influenced by the management (Hofstede, 2011). Squicciarini, Xu, and Zhang (2011) suggest that much of the literature considers "individual actions and has failed to recognize the need for privacy actions by groups" (p.522). Likewise, Wu et al. (2019) have observed that "privacy management is negotiated not just at the individual level, but between many individuals at a group or community level" (p.5). Our findings provide a new dimension and support by showing that the cultural dimension of collectivism significantly improves the enactment of privacy protective behaviors in response to privacy concerns. This finding has potential impacts for the workplace context as staff uptake of privacy protections may be encouraged by emphasizing the collectivist aspects of these protections, that is, that such protections are beneficial to the entire organization. Similarly, if the broader internet is treated as a public and shared resource, then this may encourage uptake of protective behaviors in order to safeguard this shared resource for the collective.

## Limitations and future work

This research was conducted in the midst of multiple, high-profile and heavily publicized 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 organizations to provide a "backdoor" for security agencies in Australia; and the leaking of multiple classified pieces of information by Australian security agencies (McGhee & McKinnon, 2018). In Sri Lanka, terror attacks in early 2019 prompted discussions of the effectiveness of security agencies and led to nationwide suspensions of social media services in the days immediately following the incidents. These events brought

notions of privacy, security and trust into the spotlight and may have influenced the responses in the cohort.

As noted, the variance explained by our model ($R^2$) differed substantially between Australia and Sri Lanka, which suggests that other possible determinants of acceptance of surveillance could be considered. While our work considered the role of national culture in influencing the strength of the relationship between privacy concerns and acceptance of surveillance, it is possible that cultural norms could more directly determine acceptance, and future work could measure the extent, if any, to which this is the case. Furthermore, it is possible that individual micro-cultures may have their own subset of beliefs and perceptions which could influence the results. In Sri Lanka, the Tamil group has a minority status, and this may influence factors such as their general institutional trust in the government. This is a dimension which may be explored in future work.

The method of study recruitment was through a snowball sampling, with participants initially recruited through social media. By utilizing more systematic methods of sampling and gathering information from wider areas, it would be possible to attain a larger sample of the global population, which may support the generalizability of the findings.

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

# Conclusion

As governments' capacity to subject their citizens to surveillance increases, it is reasonable to assume that so too does their desire to acquire ever greater surveillance powers. Yet there are risks to governments lacking broad public mandate for such powers. Our study found that trust in government is one of the determinants of acceptance of surveillance. While trust in government is not limited to the way in which governments manage data, it is likely that "cyber trust" is an important component of this. Dutton et al (2005) explored the role of cyber trust in government and 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 analyzed using information technologies. Through this exploration, they identified strategies which governments could employ in order to enhance levels of trust: these included ensuring trustworthy identification in online systems, implementing guidelines and legal frameworks, and the use of third party certification. It is also possible that the relationship between trust in government and acceptance of government surveillance works both ways and that a lack of acceptance of surveillance is one factor that has the ability to undermine political trust and goodwill, thereby setting up a feedback effect. Hence, methods that lead to sustained or increased acceptance of surveillance, such as increased transparency around surveillance methods and techniques, may have the potential to improve general public trust in the government.

Our study also found that privacy concerns about the collection of data were found to be a significant determinant of use of privacy protections in both cultures. In Australia, but not Sri Lanka, privacy concerns also significantly influenced acceptance of surveillance. Therefore, in Australia at least, a lack of acceptance of surveillance is more likely to result in the adoption of privacy protections which have the capacity to undermine surveillance efforts, and is therefore an important factor for governments to consider. Finally, our research found that national culture plays a role in acceptance of surveillance by influencing the extent to which some of the constructs studied influence acceptance. As such, the research contributes to a better contextual understanding of surveillance and privacy.

# References


Adams Andrew, A. (2017a). Following Snowden, German uncertainty about monitoring. *Journal of Information, Communication and Ethics in Society, 15*(3), 232-246. doi:10.1108/JICES-01-2017-0006

Adams Andrew, A. (2017b). Surveillance following Snowden: a major challenge in Spain. *Journal of Information, Communication and Ethics in Society, 15*(3), 265-282. doi:10.1108/JICES-11-2016-0044

Allison, P. 2017. "Tracking terrorists online might invade your privacy." Retrieved 2 April, 2019 from http://www.bbc.com/future/story/20170808-tracking-terrorists-online-might-invade-your-privacy

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of social issues, 33*(3), 66-84.

Associated Press. 2019. "Smart lamppost toppled to ground by Hong Kong demonstrators over Chinese surveillance fears." Retrieved 27 Aug, 2019 from https://www.abc.net.au/news/2019-08-24/hong-kong-protests-smart-lampposts-cut-down-surveillance-fears/11445606

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, F. N., Jr., & 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*, 429-472.

Bandyopadhyay, S. (2009). Antecedents and consequences of consumers online privacy concerns. *Journal of Business & Economics Research, 7*(3), 41-48.

Banisar, D., & 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*, 1.

Bennett, C. J. (2015). Trends in voter surveillance in western societies: privacy intrusions and democratic implications. *Surveillance & Society, 13*(3), 370-384.

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy, 1*(2), 243-264.

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of Internet surveillance. *European Journal of Criminology, 6*(2), 119-134. doi:10.1177/1477370808100541

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 30-57.

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change, 96*, 277-287. doi:https://doi.org/10.1016/j.techfore.2015.01.021

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42-51. doi:10.1016/j.chb.2017.12.001

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/

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28-46.

Denemark, D. (2012). Trust, efficacy and opposition to anti-terrorism police power: Australia in comparative perspective. *Australian Journal of Political Science, 47*(1), 91-113. doi:10.1080/10361146.2011.643163

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Dinev, T., & Hart, P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce, 10*(2), 7-29. doi:10.2753/jec1086-4415100201

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233. doi:10.1016/j.jsis.2007.09.002

Dutton, W., Guerra, G., Zizzo, D., & Peltu, M. (2005). The cyber trust tension in E-government: Balancing identity, privacy, security. *Information Polity, 10*(1-2), 13-23.

European Commission. 2016. "Eurobarometer survey." Retrieved 4 March, 2019 from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

European Parliament. 2016. "General Data Protection Regulation." Retrieved Feb 2, 2018 from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

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

Gormley, K. (1992). One hundred years of privacy. *Wisconsin Law Review*, 1335.

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

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Hallinan, D., & Friedewald, M. (2012). Public Perception of Modern Surveillance Technologies: A Selected Survey Analysis of the Public Perception and Acceptance of New Surveillance Technologies. *SSRN*.

Hardin, R. (2013). Government without trust. *Journal of Trust Research, 3*(1), 32-52. doi:10.1080/21515581.2013.771502

Helmreich, R. L., & Merritt, A. C. (2017). *Culture at work in aviation and medicine: National, organizational and professional influences*. New York, USA: Routledge.

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online readings in psychology and culture, 2*(1), 8.

Hofstede Insights. 2019. "Australia and Sri Lanka Country Comparison " Retrieved 15 July, 2019 from https://www.hofstede-insights.com/country-comparison/australia,sri-lanka/

Intawan, C., & Nicholson, S. P. (2018). My trust in government is implicit: Automatic trust in government and system support. *The Journal of Politics, 80*(2), 601-614. doi:10.1086/694785

Jain, R. 2019. "Biometric data breach exposes facial ID, fingerprints of millions." Retrieved 20 Aug, 2019 from https://www.ibtimes.co.uk/biometric-data-breach-exposes-facial-id-fingerprints-millions-1667951

Keil, M., Tan, B. C., Wei, K.-K., Saarinen, T., Tuunainen, V., & Wassenaar, A. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly*, 299-325.

Kluckhohn, C. (1962 ). Universal categories of culture. In S. Tax (Ed.), *Anthropology today: Selections* (pp. 304-320). Chicago, IL: University of Chicago Press (first published 1952).

MacCallum, R. C., & Browne, M. W. (1993). The use of causal indicators in covariance structure models: Some practical issues. *Psychological Bulletin, 114*(3), 533.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355. doi:10.1287/isre.1040.0032

Markus, H. R., & Kitayama, S. (1991). Culture and the self: Implications for cognition, emotion, and motivation. *Psychological Review, 98*(2), 224-253. doi:10.1037/0033-295X.98.2.224

Marx, G. T. (2015). Surveillance studies. *International encyclopedia of the social & behavioral sciences, 23*, 733-741.

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

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74. doi:10.1145/219663.219683

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

Murata, K. (2017a). Few youngsters would follow Snowden's lead in Japan. *Journal of Information, Communication and Ethics in Society, 15*(3), 197-212. doi:10.1108/JICES-08-2016-0026

Murata, K. (2017b). Following Snowden: a cross-cultural study on the social impact of Snowden's revelations. *Journal of Information, Communication and Ethics in Society, 15*(3), 183-196. doi:10.1108/JICES-12-2016-0047

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education, 15*(5), 625-632. doi:10.1007/s10459-010-9222-y

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

Parliament of the Commonwealth of Australia. 2015. "Revised Explanatory Memorandum - Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015." Retrieved 14/08/2019 from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001%22

Parliamentary Joint Committee on Intelligence and Security. (2015). *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. Retrieved from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report

Porter, C. 2018. "Speech on telecommunications legislation amendment." Retrieved 2 April, 2019 from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=CHAMBER;id=chamber%2Fhansardr%2Fb9ad0f6d-10c4-4875-a2dd-b61196fa9329%2F0016;query=Id%3A%22chamber%2Fhansardr%2Fb9ad0f6d-10c4-4875-a2dd-b61196fa9329%2F0006%22

Rainie, L., & Madden, M. 2015. "America's privacy strategies post Snowden." from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-postsnowden/

Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129-141. doi:10.1016/j.giq.2015.01.003

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

Safi, M., & Perera, A. 2018. "Sri Lanka declares state of emergency after communal violence." Retrieved 2 Feb, 2019 from https://www.theguardian.com/world/2018/mar/06/sri-lanka-declares-state-of-emergency-after-communal-violence

Shelton, M., Rainie, L., Madden, M., Anderson, M., Duggan, M., Perrin, A., & Page, D. (2015). *Americans' Privacy Strategies Post-Snowden*. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Siegrist, M., Earle, T. C., & 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), 705-716.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016. doi:10.2307/41409970

Smith, H. J., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individual's concerns about organizational practices. *MIS Quarterly, 20*(2), 167.

Smith, N., & Ferndando, S. 2019. "Sri Lanka bombings: Intelligence blunder ahead of terror attack that killed more than 200." Retrieved 5 June, 2019 from https://www.telegraph.co.uk/news/2019/04/21/sri-lanka-explosions-casualties-churches-hotels-targeted-easter/

Squicciarini, A. C., Xu, H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology, 62*(3), 521-534.

Sri Lanka Government. 2018. "President's Media Division " Retrieved June, 2019 from http://www.presidentsoffice.gov.lk/?p=5426

Suzor, N. P., Pappalardo, K. M., & McIntosh, N. (2017). The passage of Australia's data retention regime: national security, human rights, and media scrutiny. *Internet Policy Review, 6*(1), 1-16.

Thierer, A. (2013). The pursuit of privacy in a world where information control is failing. *Harvard Journal of Law & Public Policy, 36*, 409-455.

Thompson, N., & McGill, T. (2017). Mining the mind – Applying quantitative techniques to mental models of security. *Proceedings of the Australasian Conference on Information Systems 2017 (ACIS 2017), 1*(1).

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media+ Society, 3*(1), 2056305116688035.

Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421-433. doi:10.1016/j.giq.2017.07.003

Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal, 113*, 1151-1222.

Wilton, R. (2017). After Snowden – the evolving landscape of privacy and technology. *Journal of Information, Communication and Ethics in Society, 15*(3), 328-335. doi:10.1108/jices-02-2017-0010

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889-897.

Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*.

## Acknowledgement

We gratefully acknowledge the research assistants who have contributed to this project: Mr. J Kininmonth for the English survey coding and data collection, and Ms. G.Y.N Gunathilaka and Ms. T. Shanmugarajah for the Sinhalese and Tamil translations.