Cite as: Thompson, N. (2020). Government surveillance — the new normal? Privacy Law Bulletin, 17(1), 17-21.

Privacy Law
Bulletin

Government surveillance — the new normal?

Dr Nik Thompson *CURTIN UNIVERSITY*

In recent years, private citizens have found themselves subject to increasing levels of routine monitoring and surveillance. These measures are generally billed as being in the national interest, as a necessary security instrument enabling law enforcement to track criminals and prosecute crime. But the fact remains that bulk collection of information on the movements and communications of private citizens through measures such as the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) (the Act) has implications for privacy. The nature of this trade-off is recognised by lawmakers, in the words of then Prime Minister Tony Abbott: "Regrettably, for some time to come, the delicate balance between freedom and security may have to shift."[1]

There has, however, been little systematic research on the perceptions and levels of acceptance of government surveillance by citizens, and less still in an Australian context.

Background

The Act introduced a statutory obligation that service providers collect and retain communications metadata for a period of 2 years. Under s 187A(1)[2] of the Act, the following kinds of information must be kept:

- The subscriber details of a service or telecommunications device. For example, name or address information
- The source of a communication. For example, phone numbers or account identification of the service or device from which the communication has been sent
- The destination of a communication. For example, phone numbers or account identification of the telecommunications device or service
- The date, time and duration of a communication, or its connection to a relevant service. For example, accurate date and time of the start and end of the communication
- The type of communication or service used in connection with a communication. For example, if it is a voice call, SMS, email or chat message
- The location of equipment, or a line, used in connection with a communication. For example, cell network towers, Wi-Fi hotspots

When introduced as a Bill in the House of Representatives in late 2014, over 200 submissions were received and three public hearings were held. Many of the submissions from key privacy and legal bodies such as the Law Council of Australia and the Australian Human Rights Commission were critical of the scheme, in some cases declaring it incompatible with human rights and freedoms, especially those of privacy. The Parliamentary Joint Committee on Human Rights also examined the Bill, and in its report on the compatibility of the Bill with international human rights obligations stated:

> A requirement to collect and retain data on every customer just in case that data is needed for law enforcement purposes is very intrusive of privacy, and raises an issue of proportionality … The committee therefore considers that the scheme must be sufficiently circumscribed to ensure that the limitations of the right to privacy are proportionate …[3]

After the Act became law in 2015, there is evidence that members of the public may have enacted a range of methods to lawfully circumvent this government surveillance. For instance, the level of Google search activity for privacy protections such as Virtual Private Network (VPN) was seen to spike after the implementation of this metadata collection regime in Australia.[4] This data-point provides anecdotal evidence that although public debate has dwindled, levels of public acceptance of these measures may not be universal.

Australian public perceptions

To shed light on the level of public acceptance of surveillance in the Australian context, data was gathered from 100 Australian residents through an anonymous survey.[5] This is of relevance to the Australian metadata retention regime as both the success and the acceptance of this significant and costly undertaking may hinge on some of the factors being considered. Survey respondents were asked a series of questions regarding six factors. For each question, they indicated their views using a scale of 1 (Strongly Disagree) to 5 (Strongly Agree). The survey items were based on validated instruments used in prior research and the factors are summarised in the table below.

Factor	Description
Privacy concerns	Individuals' concern that data about their personalities, background or activities are being accumulated.[6]
Perceived need for surveillance	Perception that government surveillance is necessary for the protection of citizens.[7]
Trust in government	Individuals' level of trust in the government and legal system.[8]
Trust in government data management	Individuals' level of trust in the government's ability to protect data, and honesty in communicating any risks.[9]
Acceptance of surveillance	Individuals' acceptance of a range of surveillance activities.[10]
Privacy protections	Protective behaviours enacted to preserve online privacy.[11]

Only half of the respondents (52%) reported that they generally accept government surveillance. The strength of acceptance also told a similar story: on a scale from 1 (Strongly Reject) to 5 (Strongly Accept), the average response was just 3.1, meaning that respondents only weakly accept the measures.

Average privacy concerns were high (4.4 out of 5), with most respondents agreeing or strongly agreeing with the need for protection of their privacy. All other factors were generally low and tending toward slight disagreement in all cases. Lowest of all were the average levels of trust in the government's data management practices (2.4 out of 5), with many individuals believing the government is not transparent in its acquisition of, or communication about the implications of holding private data. Respondents general trust in the government (2.9 out of 5) and perceptions about the need for surveillance (2.9 out of 5) were also slightly below neutral suggesting that, on average, respondents felt a relatively low need for surveillance, and were lacking trust in the government.

When asked about their behaviours relating to privacy, respondents indicated that on average between three and four privacy protections were used out of the given list. The top three protective measures that respondents took 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 one in 10 were familiar with the anonymous communication service, "Tor".

Statistical analysis revealed that although privacy concerns do have some effect on the overall acceptance of surveillance, this is not the most influential factor. While members of the public do indicate strong views about privacy, this does not necessarily translate to a change in their views about surveillance. Instead, two different factors emerged as the strongest influences on the acceptance of surveillance. The first major influence is the perception of whether the surveillance is *needed* as a means of protecting the public. The second major influence is the general level of *trust* that the respondent places in the government.

The most influential factor is whether people believe that surveillance is necessary to protect them. This has real-world implications as legislative change is often triggered by tragic events, which may have a strong emotional impact on those involved (legislators and public alike). As time passes, the threats and associated impacts may change or diminish, but if the response has been enshrined in law its effects may be permanent.

The second most influential factor is the level of overall trust in the government. This is interesting since trust in the Australian government is generally relatively low.[12] People might be more influenced by their general view of the government than their views of specific policies and practices. If so, events that diminish that trust may also threaten the acceptance of surveillance policies.

The current environment

The Law Council has previously identified that there is potential for "function creep" when telecommunication metadata is retained and made available for an extended period "potentially allowing for information collected for one reason to be later used for other purposes".[13] While such repurposing of data may be fraught with privacy implications, in practice the situation may be much more nuanced and the possible beneficial use-cases of such data should not be overlooked.

As of April 2020, many readers will be reading this article from their own home office set up, conducting more of their business online and replacing face to face meetings with video conferences due to the COVID-19 pandemic. Many readers will also be keeping up to date on public health information through a variety of online resources, and may be deeply and personally invested in learning more about the real-world threats posed to them. With this context in mind, one point to consider if an expansion of government surveillance architecture to

support public health initiatives would be an acceptable case of such function creep.

In February 2020, the Australian Broadcasting Corporation (ABC) revealed that South Australian authorities had used phone location metadata to track the movements of two coronavirus patients who had holidayed around Adelaide. South Australian Police Commissioner Grant Stevens stated: "in this case, we think there's a genuine risk to public safety, and certainly there's community concern about this, so it's one of the occasions we elected to use it".[14] While there have been no further reports of such tracking in Australia, this approach has already been widely deployed in several countries, arguably contributing to their successful containment efforts.

Authorities in Hong Kong, Singapore, South Korea, and China extensively draw from communications metadata tracking for quarantine enforcement as well as contact tracing. In Hong Kong, those in isolation must add the border authorities' number to their WhatsApp contacts and enable the location-sharing feature. This is a setting that needs to be manually re-enabled every 8 hours, thus providing the authorities both real-time location data and the assurance that the phone is being checked regularly. Singapore and South Korea use customised apps that alert authorities if citizens stray from their permitted locations. Citizens are also advised that they must carry their phones at all times, with penalties ranging from substantial fines to the threat of jail time. In China, where the surveillance architecture is more comprehensive, it is integrated with existing private-sector platforms including the near ubiquitous WeChat and Alipay networks.

Members of the public have accepted the recent restrictions on their physical movement, possibly because the need has been well explained from a public health perspective. They might also accept increased monitoring in the digital realm for these same reasons. This would be consistent with the finding that the perceived need for surveillance has the strongest influence on acceptance. Indeed, many may argue that public health needs are a valid justification for increased digital surveillance, notwithstanding any privacy concerns.

Risks of escalation

Keeping in mind that such measures almost always involve some sort of trade-off with privacy, care must be taken to ensure that if decisions address a specific environmental context, that they should be reviewed when that environment changes. Decisions are made for one point in time but may have enduring impacts. There are two significant impediments to this re-evaluation of security measures and these can potentially lead to an escalation of surveillance over time.

Firstly, an insidious threat is the normalisation of behaviours and practices over time. This has already been observed in recent years, as surveillance has been increasingly normalised, with multiple facets of daily life subject to increased scrutiny and "datafication". Though many may still profess concern around the topic of metadata retention and even go so far as to state that they reject the measures, the level of public discourse, and media attention has faded. Even topics that may have once been viewed as a glaring affront to ones' privacy gradually start to feel normal. This is a well-understood element of human risk perception — that people tend to downplay the familiar, well known risks.[15] In practice, this can translate to a ratcheting up of surveillance while members of the public may not perceive the commensurate increase in personal risk.

Secondly, any claims of the necessity of security technology are often unfalsifiable. As new technological measures are implemented in response to a security threat, there is often no way to later re-evaluate and disprove their necessity. While claims that a security countermeasure is *sufficient* may be subject to later correction, a claim that the security countermeasure is *necessary* is not subject to such correction. In practice, if a mistake is made about a particular security measure being *sufficient* protection, then all it takes is one security issue to reveal that mistake. However, if a mistake is made about a measure being *necessary*, then no observation can reveal this error.[16] Thus mistakes can become cumulative, and lead to greater and greater levels of technical countermeasures being added over time with very few being reviewed or removed.

Conclusion

In general, members of the public are lukewarm about government surveillance — while they don't overwhelmingly accept the measures, widespread rejection has also not been observed. Interestingly, it is the general level of trust in the government and the perceptions about the need for surveillance that have the strongest influence on overall acceptance. Therefore when there is a clear public need, it is more likely that members of the public will consider increased surveillance measures to be appropriate and acceptable.

One such example where surveillance measures might be expanded is to assist public health authorities in their efforts to contain the spread of COVID-19. Though at the time of writing, widespread monitoring of physical movements has not been undertaken in Australia, the technology is already in place to do so. It is also likely that members of the public would be accepting of an increase in surveillance, provided that they are convinced of the public health need. However, any increase in the scope of surveillance in response to a short-term

situation brings the risk that when the emergency situation is over, the measures may never be removed.

There are two issues at play here that exacerbate this risk. Firstly, surveillance practices may over time become normalised, leading to a diminished risk-perception in the public. Secondly, it is often impossible to prove whether technical measures are (still) necessary for security. This can lead to a continued escalation of security countermeasures over time, and a society in which surveillance is the new normal.

Dr Nik Thompson
Senior Lecturer
Faculty of Business and Law
Curtin University
nik.thompson@curtin.edu.au
https://nikthompson.com

Footnotes

1. Commonwealth, Parliamentary Debates, House of Representatives, 22 September 2014 p 9957.
2. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), s 187A(1).
3. Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011 — Bills introduced 20 — 30 October 2014 — Legislative Instruments received 20 September — 10 October 2014* Fifteenth Report of the 44th Parliament (November 2014) para 1.31.
4. Google Trends, VPN: Australia, https://trends.google.com/trends/explore?date=2014-02-09%202018-03-12&geo=AU&q=vpn.
5. J Kininmonth et al, Privacy Concerns and Acceptance of Government Surveillance in Australia, Paper presented at the 29th Australasian Conference on Information Systems 2018, Sydney, NSW, (2018).
6. H J Smith, S Milberg and S Burke "Information privacy: Measuring individual's concerns about organizational practices" (1996) 20(2) *MIS Quarterly* 167.
7. T Dinev, P Hart and M R Mullen "Internet privacy concerns and beliefs about government surveillance — An empirical investigation" (2008) 17(3) *The Journal of Strategic Information Systems* 214.
8. E-M Trüdinger and L Steckermeier "Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany" (2017) 34(3) *Government Information Quarterly* 421.
9. M Siegrist, T Earle and H Gutscher, "Test of a trust and confidence model in the applied context of electromagnetic field (EMF) risks" (2003) 23(4) *Risk Analysis: An International Journal* 705.
10. Trüdinger and Steckermeier, above n 8.
11. Pew Research Centre, L Rainie and M Madden, Americans' Privacy Strategies Post-Snowden, 16 March 2015, www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.
12. Edelman, *2019 Edelman Trust Barometer* Global Report (2019), www.edelman.com/sites/g/files/aatuss191/files/2019-01/2019_Edelman_Trust_Barometer_Global_Report.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads.
13. Law Council of Australia, *Review of the mandatory data retention regime* (2019) para 62.
14. M Sutton "Phone tracking used to follow movements of Chinese couple with coronavirus in Adelaide" *ABC News* 6 February 2020.
15. P Slovic "The perception of risk" (1987) 236(4799) *Science* 280.
16. C Herley, "Unfalsifiability of security claims" (2016) 113(23) *Proceedings of the National Academy of Sciences of the United States of America* 6415.