Public exposure and responses to data breaches in Australia: October 2022

ANU Centre for Social Research and Methods

Professor Nicholas Biddle[1,2]; Professor Matthew Gray[1]; and Associate Professor Steven McEachern[1,3]

1 ANU Centre for Social Research and Methods Australian National University

2 National Data Advisory Committee

3 Australian Data Archive

8th November, 2022

Abstract

This paper reports Australian's views about data trust, cybercrime and data breaches and how these have changed. It is based on data from four waves of the ANUpoll collected over the period October 2019 to October 2022 with the two most recent waves being collected between the 8th and 22nd of August, and the 10th and the 24th of October. This allows the estimation of the short-run impacts of a major and high-profile data breach of data held by a major Australia telecommunication company in September 2022 on Australians trust in various institutions to maintain data privacy and how various groups should be able to use data.

Almost one-third of Australians report that they had been exposed to a data breach in the previous 12-months. Trust in key institutions and types of organisations with regards to data privacy declined quite substantially between August and October 2022, though on average across eight types of institutions/organisations trust still remained higher than pre-COVID-19. The largest decline across the eight types of institutions/organisations asked about in the survey was for telecommunications companies, which is not surprising given the September 2022 data breach was of data held by Optus Telecommunications. There was also a decline in trust in companies that people use to make purchases online, universities and other academic institutions, as well as the Australian Bureau of Statistics.

We do not find much evidence that specific concerns about cybercrimes increased in the twelve months to October 2022. There is some evidence, however, that those who have experienced a data breach themselves have become more likely to be 'very concerned' about identity theft. However, between October 2021 and 2021 there was a large increase in the per cent of Australians who thought that governments should intervene with regards to companies' use of data and a decline in the per cent of Australians who thought that companies are better equipped to protect their data or that it was up to consumers themselves.

Acknowledgements

The ANU Centre for Social Research and Methods COVID-19 Impact Monitoring series has received funding from the Australian Institute of Health and Welfare. The authors would like to particularly thank Matthew James, Deputy CEO Australian Institute of Health and Welfare, for comments on reports and survey instruments in this series. The opinions and conclusions in this paper should, however, be attributed to the authors only. The survey data will be available for download through the Australian Data Archive (http://dx.doi.org/10.26193/FCZGOK)

1 Introduction

On the 22nd of September, 2022, the major Australian telecommunications company Optus revealed that a data breach resulted in what may end up being over 10 million customers having their personal data stolen. For a very large proportion of these customers, sensitive information may have been released, including passport, Medicare and licence numbers.[1] Not long after the breach, a person by the name of 'Optusdata' published two samples of data and over 10,000 records, threatening to release similar numbers of records each day unless they received payment of $1million from Optus.[2] The records have subsequently been removed, but at the time of writing the person or persons who accessed data from the Optus system has not been identified, and there is still a real possibility that customer records will be used as part of ongoing criminal activity.

The Optus data breach was not the first and will nor will it be the last data breach affecting Australians. The Australian National University, internet company Canva,[3] and most recently Medibank (Australia's largest health insurer)[4] to name a few have all suffered large-scale data breaches, varying in degree of sophistication, number of people affected, and sensitivity of data obtained.

More broadly, the Australian Cyber Security Centre in its *Annual Cyber Threat Report* for July 2021 to June 2022[5] noted that the last year saw 'an increase in the number and sophistication of cyber threats, making crimes like extortion, espionage, and fraud easier to replicate at a greater scale.' Furthermore, the report notes that 'In 2021–22, ransomware groups stole and released the personal information of hundreds of thousands of Australians as part of their extortion tactics. The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers.'

The Australian Government responded quickly to the Optus data breach. They provided a factsheet (still being updated) that provides resources for affected customers, and have made it clear that Medicare cards and passports can be replaced either free of charge or reimbursed by Optus, with state/territory governments providing similar assurances with regards to licences. Some of the changes are more substantive though and are designed to minimise the amount of data that companies like Optus feel they need to hold on their customers. Specifically:

> *'The amendments will enable telecommunications companies to temporarily share approved government identifier information (such as drivers licence, Medicare and passport numbers of affected customers) with regulated financial services entities to allow them to implement enhanced monitoring and safeguards for customers affected by the data breach.'*[6]

There is a large and growing body of literature detailing the effect of data breaches on the companies holding records. The findings of this research are mixed. Juma'h and Alnsour (2020) conclude that their analysis 'does not confirm a relationship between data breaches and … quarterly changes in share prices' and Makridis (2021) shows that not all data breaches have a negative impact and that 'firms experience a 26–29% increase in reputational intangible capital following an average data breach.' An important finding from Makridis (2021) though is that 'the largest and most salient breaches are associated with a 5–9% decline in reputational intangible capital following a data breach.' Chen and Jai (2019) also show that data breaches impact differently on customer perceptions depending on whether the customer has some ongoing attachment to the company (for example as a loyalty member). The response of

companies also matters, with Muzatko and Bansal (2018) showing that 'companies that delay the announcement of a data breach are likely to suffer a larger drop in consumer trust than those companies that immediately disclose the data breach.'

There is less information available, however, of the impact of large data breaches on national-level attitudes. This is partly because such data is not routinely collected in nationally representative samples. Since October 2018, the ANU Centre for Social Research and Methods has been monitoring attitudes to data trust and data privacy, through the ANUpoll series of surveys. A number of questions in the wave of data collection just prior to the data breach (August 2022) focused on data trust and data privacy and questions were also included in the May 2020 and August 2021 waves. The October 2022 wave (the 53rd wave of ANUpoll,), partly in response to the Optus data breach, but also as part of the long-running series of questions on cybercrime, some of the questions from the August 2022 ANUpoll and previous waves of data collection were repeated, and a number of new questions were asked. Data collection for the October 2022 ANUpoll was undertaken between the 10th and 24th of October 2022.[7] There were a total of 3,468 respondents.

Analysis of the ANUpoll data up to and including the August 2022 data found that trust in key institutions and types of organisations with regards to data privacy increased during the early stages of COVID-19 period, and has remained high through to mid-2022 (Biddle et al. 2022). Biddle et al. (2022) conclude that

> *'Australians also for the most part think governments should be sharing data with researchers (particularly in universities) and making use of data internally. However, support for such uses of data is slipping… [and] a low percentage of Australians and fewer Australians than in 2018 agreed that governments 'could respond quickly and effectively to a data breach' – down from 34.0 per cent in October 2019 to 30.3 per cent in August 2022'*

This paper provides a summary of data from the October 2022 survey, making comparisons with previous waves of data collection. In Section 2 of the paper, we look at who has been exposed to data breaches whereas in Section 3 we attempt to understand the impact of data breaches on trust in key institutions and types of organisations. We then look at cybercrimes more broadly (Section 4) and views on policy responses (Section 5). In Section 6 we provide some concluding comments.

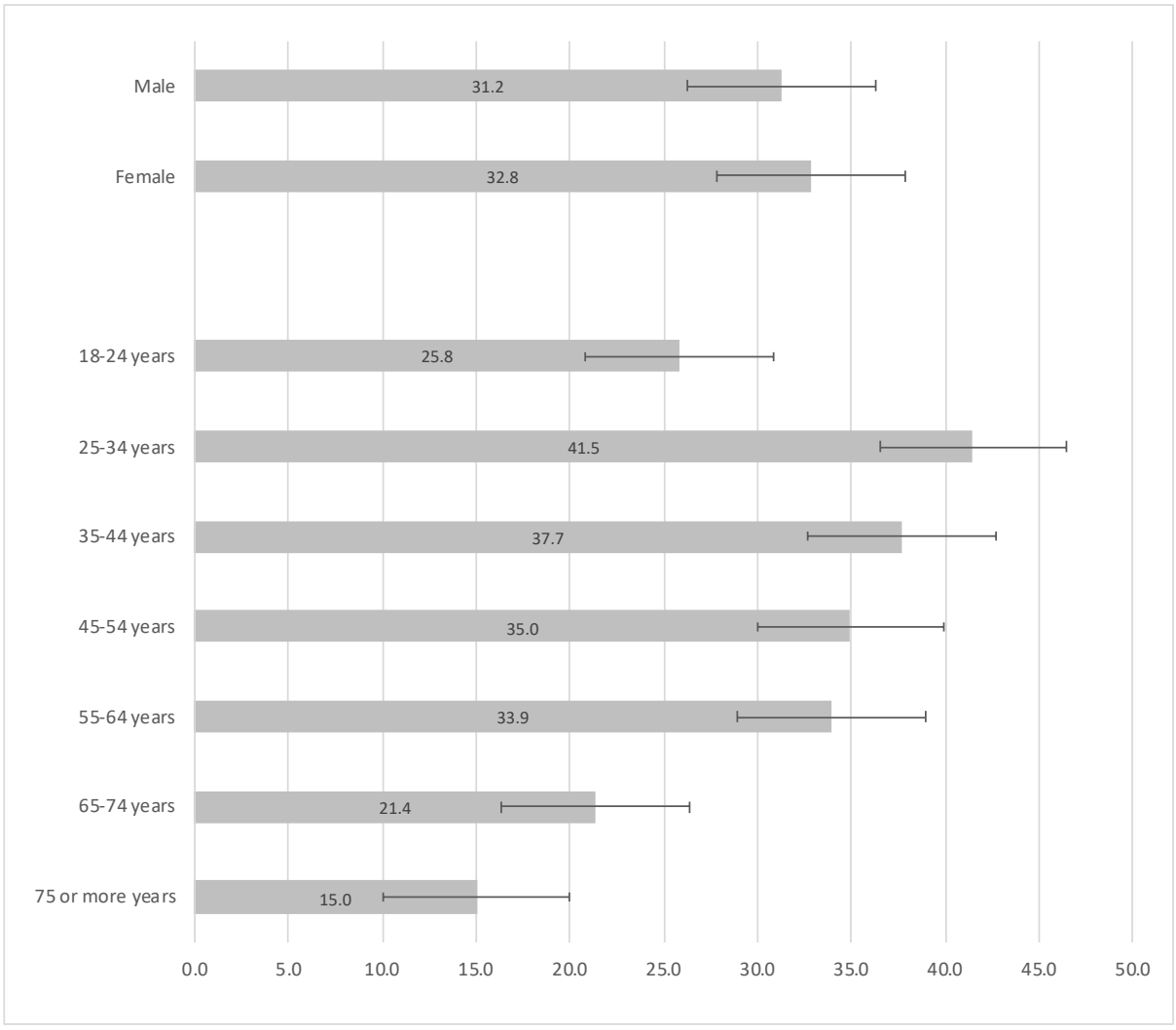
2 Who has been exposed to data breaches

The October 2022 ANUpoll included the question 'Have you, or a member of your household, been the victim of a data breach in the last 12 months?'. One-third (32.1 per cent) of households, according to this data, had experienced a data breach in the last 12 months, Responses to this question are likely to understate the extent to which people experience a data breach because in many cases not everyone whose personal data has been the subject a data breach will be aware of this. The roughly one-third of households that have been exposed in the last 12 months is therefore likely to be an underestimate of the number of household affected, but is nonetheless far higher than the 11.2 per cent of Australians who reported that they or a member of their household had been the victim of a burglary or assault in the previous 5 years (reported in the same October 2022 ANUpoll).

The household exposure nature of the question needs to be taken into account when interpreting demographic differences in experience of data breaches

Men and women report a very similar rate of living in a household in which a member(s) had experienced a data breaches (Figure 1). There, however, are quite large age differences in exposure to data breaches. The age group living in households with the greatest exposure to data breaches is those aged 25 to 34 years, with 41.5 per cent reporting that they or their household had been exposed in the previous 12 months. Rates are also quite high for those aged 25 to 64 years, with younger Australians aged 18 to 24 (25.8 per cent) and older Australians aged 65 to 74 (21.4 per cent) and particularly aged 75 years and over (15.0 per cent) having low rates of exposure.

Figure 1 Australians whose household has been exposed to a data breach in the previous 12-months, by age and sex, October 2022



Note: The “whiskers” on the lines indicate the 95 per cent confidence intervals for the estimate.

Source: ANUpoll: October 2022.

A regression model is estimated to help understand the factors associated with the probability of living in a household which had been exposed to a data breach. Because the dependent variable is binary, a probit model is estimated. Explanatory variables include demographic, socioeconomic, and geographic factors.

The estimates from the regression model confirm these age patterns hold when other factors are controlled. However, there are a number of other demographic, socioeconomic, and

geographic factors that are associated with being a victim of a data breach. Those who were born overseas in a non-English speaking country were less likely to report that they had been a victim of a data breach, as were those who lived in a non-capital city. Specifically, without controlling for other factors, those who live in a capital city were 6.6 percentage points more likely to have been a victim of a data breach (34.3 per cent) than those who live outside of a capital city (27.7 per cent).

There is a reasonably complex relationship between household income and exposure to data breaches. This is true whether we examine average differences or whether we control for other factors. The lowest probability in the regression analysis is for those in the middle income category, with higher probabilities for those in the second and fifth income quintile. Socioeconomic advantage does not appear to protect people from data breaches.

Table 1 Demographic, geographic, and socioeconomic factors associated with living in a household which had been exposed to a data breach in the previous 12 months, October 2022

Explanatory variables	Coeff.	Statistical significance
Female	0.035	
Aged 18 to 24 years	-0.331	**
Aged 25 to 34 years	0.066	
Aged 45 to 54 years	-0.112	
Aged 55 to 64 years	-0.069	
Aged 65 to 74 years	-0.402	***
Aged 75 years plus	-0.740	***
Indigenous	-0.033	
Born overseas in a main English-speaking country	-0.003	
Born overseas in a non-English speaking country	-0.258	**
Speaks a language other than English at home	0.032	
Has not completed Year 12 or post-school qualification	-0.194	
Has a post graduate degree	-0.035	
Has an undergraduate degree	-0.127	
Has a Certificate III/IV, Diploma or Associate Degree	-0.027	
Lives in the most disadvantaged areas (1st quintile)	0.018	
Lives in next most disadvantaged areas (2nd quintile)	-0.065	
Lives in next most advantaged areas (4th quintile)	0.024	
Lives in the most advantaged areas (5th quintile)	-0.015	
Lives outside of a capital city	-0.153	**
Lives in lowest income household (1st quintile)	0.024	
Lives in next lowest income household (2nd quintile)	0.223	**
Lives in next highest income household (4th quintile)	0.098	
Lives in highest income household (5th quintile)	0.180	*
Constant	-0.270	*
Sample size	3,122	

Notes: Probit regression model. The base case individual is male; aged 35 to 44 years; non-Indigenous; born in Australia; does not speak a language other than English at home; has completed Year 12 but does not have a post-graduate degree; lives in neither an advantaged or disadvantaged suburb (third quintile); lives in a capital city; lives in neither a high-income or low-income household (third quintile).

Coefficients that are statistically significant at the 1 per cent level of significance are labelled ***; those significant at the 5 per cent level of significance are labelled **, and those significant at the 10 per cent level of significance are labelled *

Source: ANUpoll October 2022

3 Trust in institutions and types of organisation regarding data privacy

The direct impact of data breaches is generally felt most acutely by those whose data is accessed, as well as by the companies/organisations that are breached. However, data breaches can also have flow-on impacts to the broader community by reducing trust in key institutions and types of organisations, and by requiring customers/companies to take ever more expensive and intrusive preventative measures. We can clearly see this decline in trust by comparing responses to a repeated question we have asked on the ANUpoll since October 2018, and repeated in the October 2022 survey (as well as May 2020, August 2021, and August 2022).

Respondents were asked: 'On a scale of 1 to 10, where 1 is no trust at all and 10 is trust completely, how much would you trust the following types of organisations to maintain the privacy of your data?'. Respondents were asked about eight types of organisations as listed below, and the order in which the organisations were presented to the respondent was randomised:

a) The Commonwealth Government in general
b) The State / Territory Government where you live
c) Banks and other financial institutions
d) Social media companies (for example Facebook, Twitter, Google)
e) Universities and other academic institutions
f) Telecommunications companies
g) Companies that you use to make purchases online
h) The Australian Bureau of Statistics

For some analyses, it is useful to have a combined measure of trust across multiple types of institutions/organisations. A principal components analysis suggests that a measure of trust in institutions/organisations through a single index with equal weights is appropriate.[8] Therefore the index of trust in data privacy is simply the average value of trust in the eight institutions asked about. A higher value of the index indicating that the individual has a higher overall level of trust in the ability of the different types of organisations to maintain their data privacy.

Biddle et al. (2022) using data from October 2018 to August 2022 find that 'Following an increase in the overall level of trust in a range of types of organisations to maintain data privacy between October 2018 and May 2020 from 4.78 to 5.70, there was a decline between May 2020 and August 2021 to 5.49.' Although there had been no statistically significant change between August 2021 and August 2022 (when the average value was 5.50), there was a large and significant decline over the two months that follows, with the index of trust falling to 5.27 in October 2022.

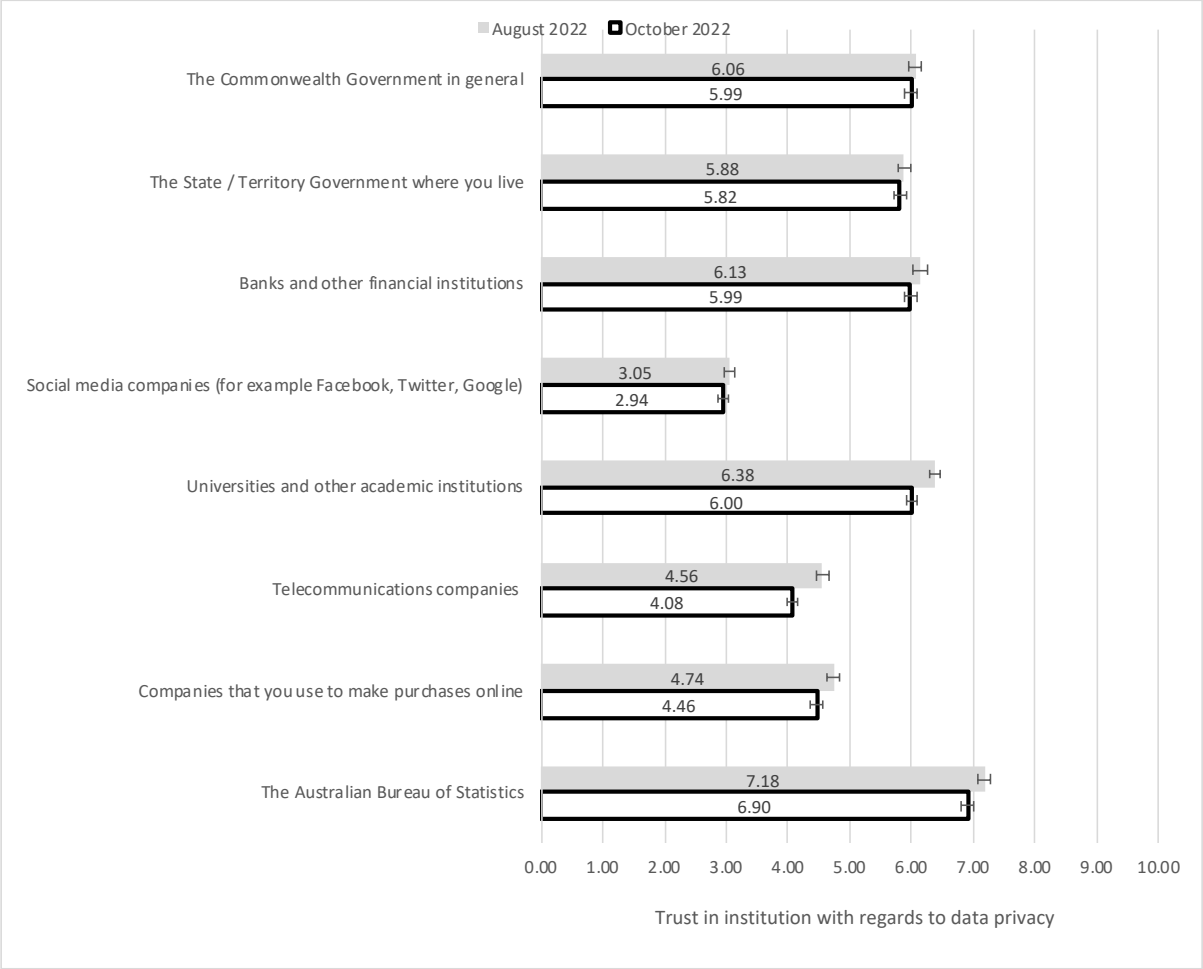
Taking a slightly longer term perspective, the decline in trust between August 2021 and October 2022 was greater for those who reported that they or someone in their household had been a victim of a data breach than those who had not. For those who hadn't been a victim of a data breach and completed both surveys, the index of trust fell from 5.58 to 5.39. For those who had been a victim, however, the decline was much greater – from 5.37 in August 2021 to 5.04 in October 2022.

Not surprisingly, given the nature of the data breach most front-of-mind in October 2022, the decline in data trust was much greater when it comes to telecommunications companies.

Specifically, as shown in Figure 2, there was a 10.5 per cent decline in the average trust in telecommunications companies between August and October 2022 – from 4.56 to 4.08. Importantly though, trust in telecommunications companies still remains above what it was pre-COVID-19 (3.73, as reported in Biddle et al. 2022).

Not all types of institutions and organisations experienced a decline in trust between August and October 2022, with no difference between those two months in trust with regards to the Commonwealth government; State/Territory governments; banks and other financial institutions; and social media companies. There were, however, three other sets of institutions that experienced a decline in trust over the period, despite not seeming to have been directly involved in any recent data breaches. There was a decline in trust for universities and other academic institutions (from 6.38 to 6.00), online companies (from 4.74 to 4.46) and the Australian Bureau of Statistics (from 7.18 to 6.90). It may have been a coincidence that trust declined for these institutions, and it may have been unrelated to any recent data breaches. However, the results do show that even in the absence of any specific data breach, trust can still decline over a relatively short period of time.

Figure 2 Average level of trust in institutions/types of organisations to maintain data privacy – August to October 2022



Note: The "whiskers" on the lines indicate the 95 per cent confidence intervals for the estimate.

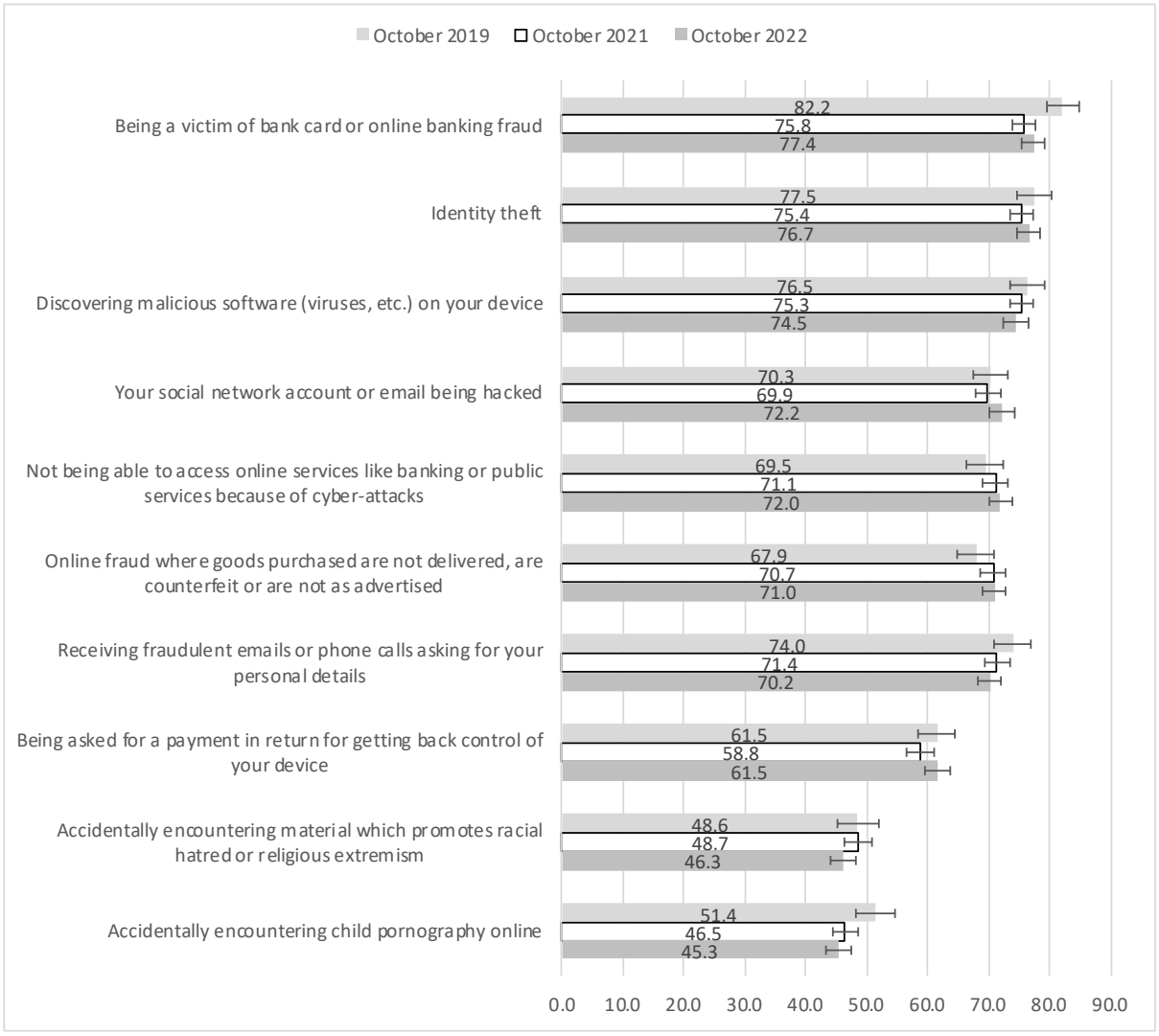
Source: ANUpoll: August and October 2022.

4 Concerns about cybercrime

Despite the very public data breach that occurred just prior to the October 2022 survey, there does not appear to have been a noticeable increase in the proportion of Australians who are concerned about specific types of cybercrimes. In October 2019, 2021, and 2022, respondents were first reminded that 'Cybercrimes can include many different types of criminal activity.' They were then asked 'How concerned are you personally about experiencing or being a victim of the following situations…?' with 10 potential situations asked about. Figure 3 gives the proportion of Australians who were very or fairly concerned in each of those three waves, ordered by the situation that respondents were most concerned about as of October 2022.

A very large proportion of Australians were fairly or very concerned about a range of cyber-crimes, in particular being a victim of bank card or online banking fraud (77.4 per cent), identity theft (76.7 per cent) and discovering malicious software on their device (74.5 per cent). However, none of these experienced an increase in concern over the period.

Figure 3 Per cent of Australians fairly concerned or very concerned about specific cybercrime situations –October 2019, 2021, and 2022



Note: The "whiskers" on the lines indicate the 95 per cent confidence intervals for the estimate.

Source: ANUpoll: October 2019, October 2021, and October 2022.

Although in general there does not appear to be much evidence that overall levels of concern have gone up with regards to cyber-crimes, there is some evidence that those who have been a victim of a data breach have become more concerned about identity theft. Specifically, in October 2021 there was no difference in the per cent of those who were very concerned about data theft between those who would end up being a victim of a data breach (according to the October 2022 survey) and those who wouldn't (37.5 and 35.8 per cent respectively). When asked again in October 2022, however, 44.6 per cent of those who had been a victim of a data breach over the previous 12 months were very concerned about identity theft, compared to 36.2 per cent of those who had not been a victim of a data breach. It would appear that individual or household-level exposure to data breaches increases concerns about identity theft, but there is no change for the population more broadly.

5 Policy responses to data breaches

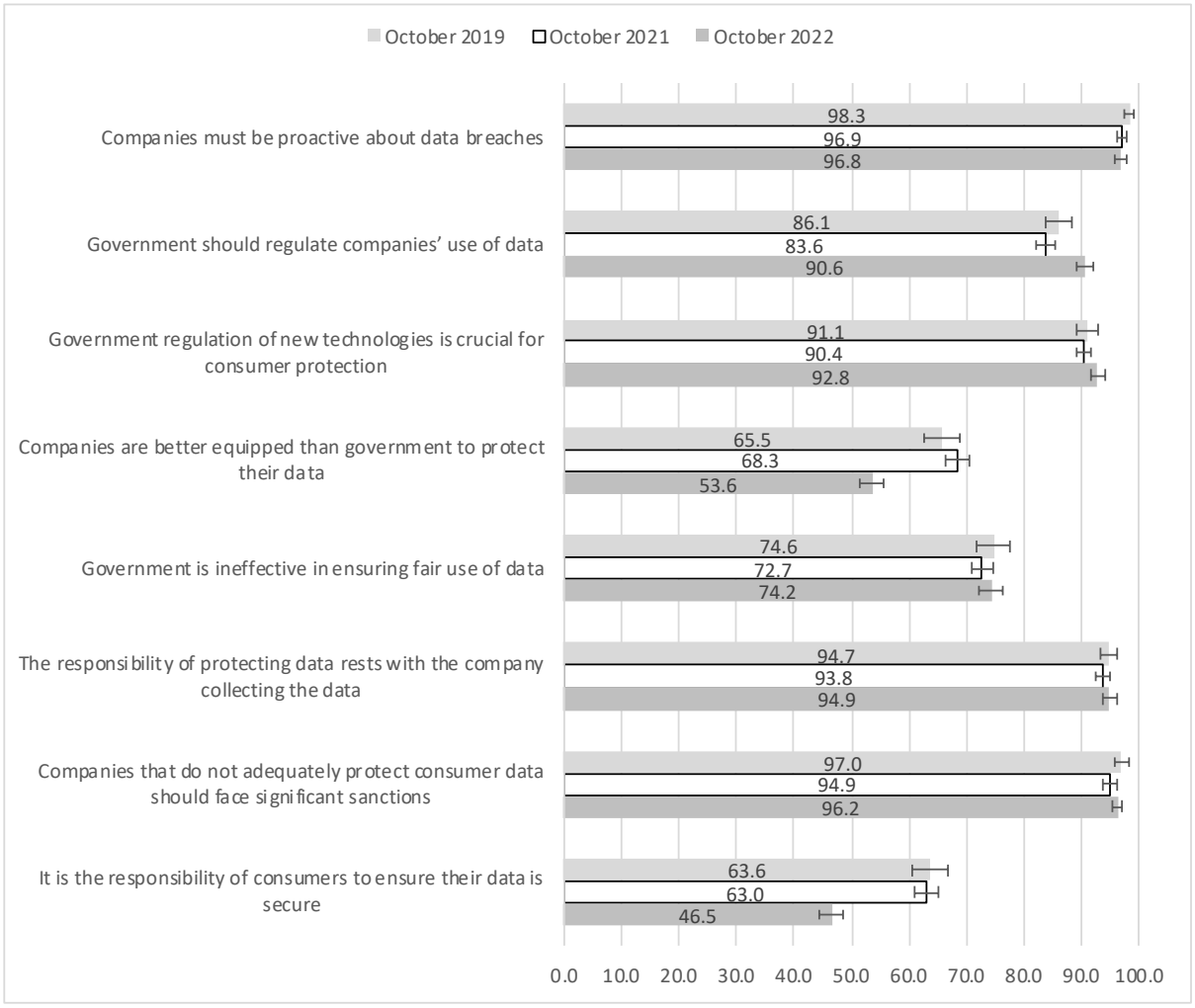
The Australian government was quick to respond to the Optus data breach. The Hon. Clare O'Neil, the Minister for Cyber Security and Home Affairs, has also made a number of public statements, including:

> *"Optus needs to communicate clearly to the Australian Government, and to their customers, about exactly what information has been taken regarding specific individuals. This will enable us to make sure that those 10 million Australians who have had some of their personal information stolen are not at risk of some type of financial crime or online fraud. The Albanese Government is completely focused on trying to protect all those people affected by the theft of their information which is unprecedented in Australian history. This is a security breach that should not have occurred, but what's really important here is that we row in the same direction and do everything we can to stop financial crime against Australians. We urge Optus do everything it can to provide our agencies with the information they need to help us do that."*[9]

When we compare the responses across the October 2019, 2021, and 2022 surveys to a series of questions on data breaches, it is clear that the policy changes made leading up to the most recent data collection was not sufficient from the public's perspective. Specifically, Figure 4 gives the per cent of Australians who totally agree or tend to agree with each of eight statements, when asked in each of the three years.

Between October 2019 and 2021 there was a reasonable level of stability regarding views on data breaches. However, in the 12 months that followed, attitudes changed substantially to be more supportive of government intervention and less supportive of companies themselves. Specifically, the largest increase over the period was for the per cent of Australians who thought that government should regulate companies' use of data (from 83.6 to 90.6 per cent), but also a small increase in the per cent of Australians who thought that government regulation of new technology is crucial for consumer protection (from 90.4 to 92.8 per cent). Using the opposite framing, there was a very large decrease in the percent of Australians who thought that it was the responsibility of consumers to ensure their data is secure (from 63.0 to 46.5 per cent) and an almost as large decrease in the per cent of Australians who thought that companies are better equipped than government to protect their data (68.3 to 53.6 per cent).

Figure 4 Per cent of Australians who totally agree or tend to agree with statements regarding data breaches – October 2019, 2021, and 2022



Note: The "whiskers" on the lines indicate the 95 per cent confidence intervals for the estimate.

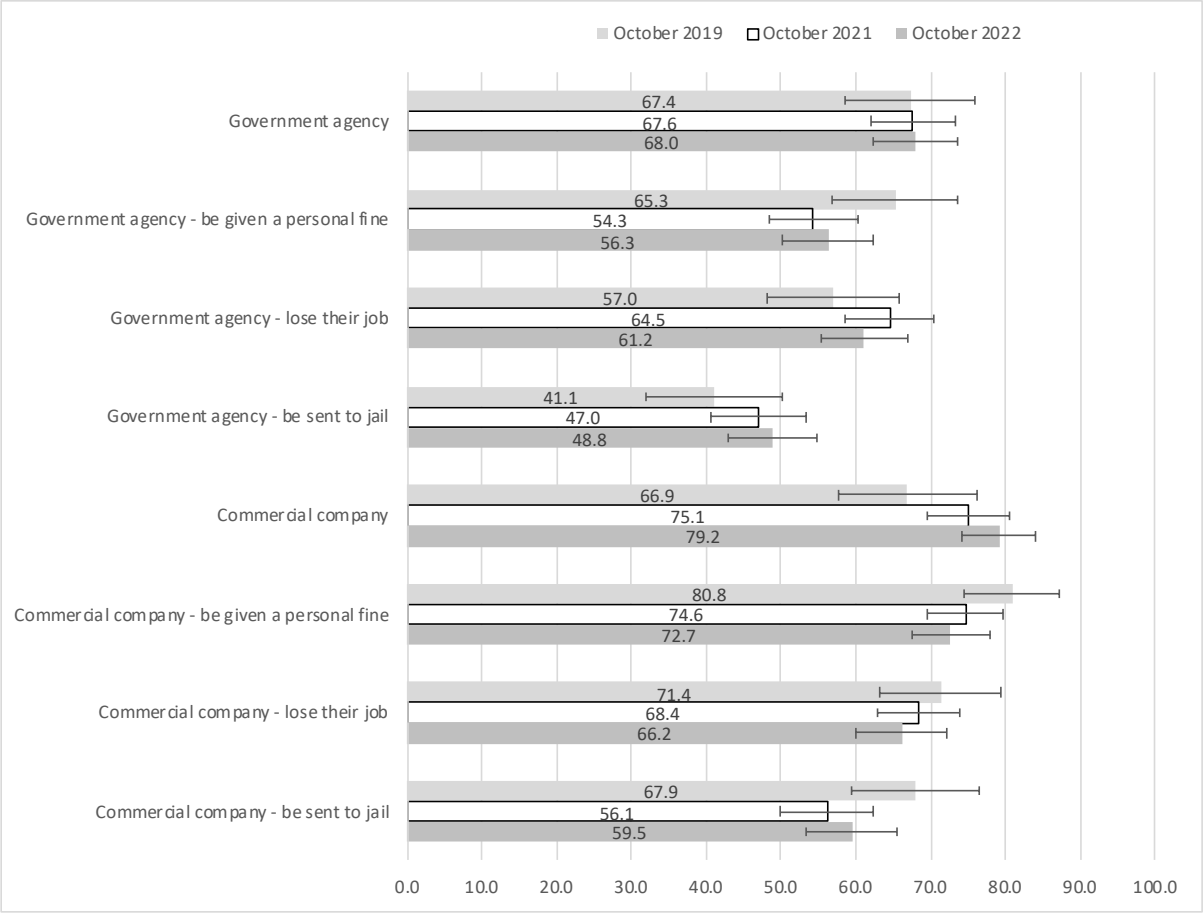
Source: ANUpoll: October 2019, October 2021, and October 2022.

The final question asked in the module was with regards to who should be held responsible for a serious data breach. For half the sample, we asked about whether the head of a government agency should be held personally responsible, and for the other half of the sample we asked whether the head of a commercial company should be held responsible. Within each of these two groups, one quarter of respondents were just asked about whether they should be held responsible. However, the remainder were split into three groups (with a quarter of the sample each) and asked whether the head of the agency/company be given a personal fine, lose their job, or be sent to jail. Figure 5 give the per cent of Australians who totally agree or tend to agree based on each of these combinations, for October 2019, 2021, and 2022.

There is considerable uncertainty around the estimates, because of the random splitting of the sample which reduces the sample size for the estimates. However, some interesting and important patterns and trends emerge. In general, for all three years, Australians were more likely to think that the head of a commercial company should be held responsible compared to the head of a government agency. Australians were also less likely to think that heads of agencies/companies be sent to jail compared to other actions, though there was still 59.5 per cent of Australians (in October 2022) who thought that the head of a commercial company

should be sent to jail and 48.8 per cent who thought the head of a government agency be sent to jail. Trends through time are a bit harder to distinguish, though there is some evidence that Australians are increasingly likely to think that the head of a commercial company should be held personally responsible, increasing from 66.9 per cent in October 2019 to 79.2 per cent in October 2022 when the specific penalty is not stated.

Figure 5 Per cent of Australians who totally agree or tend to agree with statements regarding personal responsibility for data breaches – October 2019, 2021, and 2022



Note: The "whiskers" on the lines indicate the 95 per cent confidence intervals for the estimate.

Source: ANUpoll: October 2019, October 2021, and October 2022.

6 Concluding comments

There is evidence that over the last one to two decades, data breaches are becoming more common, or at the very least are becoming more likely to be reported by the companies that are exposed to them (Edwards et al. 2016). In the survey analysis presented in this paper, a little under one-third of Australians had been exposed to a data breach in the year prior to October 2022.

While the impact of data breaches on companies is mixed and non-linear (Makridis 2021), collectively very large data breaches have the potential to undermine trust in the system as a whole, rather than just individual companies. In September 2022 the Australian telecommunications company Optus announced a very large data breach, with records of more than 10 million customers (about 40 per cent of the Australian population) accessed,

including many records that contained very sensitive information that could be used to enable identity theft.

In August 2021 just prior to the announcement of the data breach, a number of questions were asked on a representative sample of the Australian population on trust in key institutions with regards to data privacy. These questions had been asked a number of times since October 2018, with specific questions on cybercrimes and data breaches also asked in October 2019 and 2021. In October 2022, immediately after the announcement of the data breach, these questions were repeated using the same longitudinal panel, providing what we believe to be the first longitudinal data on a representative sample of a national population with relevant information just prior to and just after a national-level data breach.

Analysis of the data suggests that trust in key institutions and types of organisations declined quite substantially between August and October 2022, though on average across eight institutions trust still remained higher than pre-COVID-19. Not surprisingly, the largest decline across the eight institutions/types of organisation asked about in the survey was for telecommunications companies, with declines also for companies that people use to make purchases online. Somewhat positively, trust in a number of institutions does not appear to have been impacted by the Optus data breach, including the Commonwealth government, and State/Territory governments.

An important finding is that trust in universities and other academic institutions and the Australian Bureau of Statistics declined. This is despite these institutions being seemingly unrelated to Optus or the type of data breach that occurred in September 2022. It may be that there were other factors or events that occurred between August and October 2022 that explains these declines. However, it may also be that the Optus data breach reminded the Australian public of data breaches that had occurred at Australian universities in the past, or the difficulties that the Australian Bureau of Statistics had with the 2016 online Census form (when it should be noted no data breach actually occurred).

We do not find much evidence that specific concerns about cybercrimes increased in the twelve months to October 2022. There is some evidence, however, that those who have experienced a data breach themselves have become more likely to be 'very concerned' about identity theft.

A key finding from the analysis was that between October 2021 and 2021 there was a large increase in the per cent of Australians who thought that governments should intervene with regards to companies' use of data and a decline in the per cent of Australians who thought that companies are better equipped to protect their data or that it was up to consumers themselves. While the survey did not ask about specific interventions, since the Optus data breach there have been calls for mandatory disclosure laws[10] as well as limits on how much data can be collected from customers and for how long that information can be retained.[11]

There are clearly risks involved in such legislation, particularly with regards to firm profitability and the consumer experience. However, the Australian public would seem to be increasingly of the view that the benefits of stronger legislation far outweigh the costs, with the negative externalities experienced by other institutions between August and October 2022 providing support for such a case.

References

Biddle, N., Gray, M., and McEachern, S., (2022). *Data trust and data privacy: A brake on the data and digital dividend?* https://csrm.cass.anu.edu.au/research/publications/data-trust-and-data-privacy-brake-data-and-digital-dividend

Chen, H.S. and T.M. Jai (2021). 'Trust fall: Data breach perceptions from loyalty and non-loyalty customers.' *The Service Industries Journal*, 41(13-14):947-963.

Edwards, B., S. Hofmeyr and S. Forrest (2016). 'Hype and heavy tails: A closer look at data breaches.' *Journal of Cybersecurity*, 2(1):3-14.

Juma'h, A.H. and Y. Alnsour (2020). 'The effect of data breaches on company performance.' *International Journal of Accounting & Information Management*, 28(2): 275-301.

Makridis, C.A., (2021). 'Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018.' *Journal of Cybersecurity*, 7(1), p.tyab021.

Appendix 1 Describing the data

In April 2020, the Social Research Centre on behalf of the ANU Centre for Social Research and Methods collected the first wave of data as part of the centre's COVID-19 Impact Monitoring Series.[12] Since that first wave of data collection, surveys have been undertaken a further 12 times, with the most recent wave of data collection undertaken in October 2022.

Between the 1st and 13th wave of data collection for the COVID-19 Impact Monitoring series, there have been 6,537 adult Australians that have answered at least one of the surveys, with 1,341 answering all surveys.

Surveys have also been conducted with the same group of respondents in January and February 2020, just before the COVID-19 pandemic started in Australia, as part of the ANUpoll and Australian Social Survey International-ESS (AUSSI-ESS) surveys respectively.[13] This allows us to track outcomes for the same group of individuals from just prior to COVID-19 impacting Australia through to two-and-a-bit years since COVID-19 first reached Australia.

The October 2022 survey collected data from 3,468 Australians aged 18 years and over.[14] Data collection for this most recent ANUpoll commenced on the 10th of October 2022 with a pilot test of telephone respondents. The main data collection commenced on the 11th and concluded on the 24th of October. 57.3 per cent of the sample had completed the survey by the 13th of October and the average interview duration was 27.4 minutes.

The Social Research Centre collected data online and through Computer Assisted Telephone Interviewing (CATI) in order to ensure representation from the offline Australian population. Around 2.8 per cent of interviews were collected via CATI.[15] A total of 4,280 panel members were invited to take part in the October 2022 survey, leading to a wave-specific completion rate of 81.0 per cent.[16]

Data in the paper is weighted to population benchmarks. For Life in Australia™, the approach for deriving weights generally consists of the following steps:

1. Compute a base weight for each respondent as the product of two weights:
    a. Their enrolment weight, accounting for the initial chances of selection and subsequent post-stratification to key demographic benchmarks
    b. Their response propensity weight, estimated from enrolment information available for both respondents and non-respondents to the present wave.
2. Adjust the base weights so that they satisfy the latest population benchmarks for several demographic characteristics.

Across all thirteen surveys undertaken during the COVID-19 period, there were 6,690 respondents that completed at least one of the waves of data collection. 18.3 per cent of these completed one wave of data collection only, with a further 7.4 per cent having completed two waves. At the other end of the distribution, 20.5 per cent of the cumulative respondents completed all thirteen waves of data collection and a further 6.3 per cent completed twelve of the thirteen waves.

Table 1 gives the number of respondents for each of the thirteen waves of data collection during the COVID-19 period, as well as the two pre-COVID waves. The table also gives the survey window for the data collection, and the per cent of January 2020 respondents who completed that particular wave. In between the April and August 2022 surveys, the

Comparative Study of Electoral Systems (CSES) survey was undertaken on the Life in Australia™ panel, with a limited range of data items available for analysis in this paper.

Table A1 Survey participation – January 2020 to April 2022

Wave	Survey window	Sample size	Per cent of January 2020 survey that completed wave
January 2020	20th January to 3rd February, 2020	3,249	100
February 2020	17th February to 2nd March, 2020	3,228	91.4
1 – April 2020	14th to 27th April, 2020	3,155	88.8
2 – May 2020	11th to 25th May, 2020	3,249	91.0
3 – August 2020	10th to 24th August, 2020	3,061	85.9
4 – October 2020	12th to 26th October, 2020	3,043	85.5
5 – November 2020	9th to 23rd November, 2020	3,029	84.9
6 – January 2021	18th January to 1st February, 2021	3,459	83.8
7 – April 2021	12th to 26th April, 2021	3,286	80.8
8 – August 2021	10th to 23rd August, 2021	3,135	71.1
9 – October 2021	12th to 26th October, 2021	3,474	68.6
10 – January 2022	17th to 30th January, 2022	3,472	63.4
11 – April 2022	11th to the 24th of April, 2022	3,587	64.0
CSES	23rd May to 5th June, 2022	3,556	63.5
12 – August 2022	8th to 22nd August, 2022	3,510	62.7
13 – October 2022	10th to 24th October, 2022	3,468	62.4

Endnotes

1 https://www.bbc.com/news/world-australia-63056838
2 https://www.gizmodo.com.au/2022/09/optus-data-breach-details/
3 https://www.upguard.com/blog/biggest-data-breaches-australia
4 https://www.theguardian.com/technology/2022/oct/26/medibank-confirms-all-39-million-customers-had-data-accessed-in-hack
5 https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf
6 https://ministers.treasury.gov.au/ministers/jim-chalmers-2022/media-releases/changes-protect-consumers-following-optus-data-breach
7 The data is available for download through the Australian Data Archive (DOI: 10.26193/WBJE1K) with more information on the data available in Appendix 1.
8 The Eigenvalue for the first component is 4.66 (explaining 58.3 per cent of the variation) and the Eigenvalue for the second component is 1.12. All eight of the variables correlated at a similar level with the first component (minimum Eigenvalue of 0.27 and a maximum of 0.40).
9 https://ministers.dss.gov.au/media-releases/9256
10 https://theconversation.com/after-the-optus-data-breach-australia-needs-mandatory-disclosure-laws-192612
11 https://theconversation.com/optus-data-breach-regulatory-changes-announced-but-legislative-reform-still-needed-192009
12 https://csrm.cass.anu.edu.au/research/publications/covid-19
13 The ANUpoll series of surveys is collected on a probability-based, longitudinal panel (Life in Australia™). By using probability-based recruiting (predominantly telephone-based) the unknown and unquantifiable biases inherent in opt-in (non-probability) panels are minimised and it is also possible to quantify the uncertainty around the estimates due to sampling error using standard statistical techniques. This is not possible with non-probability surveys.
14 The unit record survey data is available for download through the Australian Data Archive (http://dx.doi.org/10.26193/FCZGOK).
15 The contact methodology adopted for the online Life in Australia™ members is an initial survey invitation via email and SMS (where available), followed by multiple email reminders and a reminder SMS. Telephone follow up of panel members who have not yet completed the survey commenced in the second week of fieldwork and consisted of reminder calls encouraging completion of the online survey. The contact methodology for offline Life in Australia™ members was an initial SMS (where available), followed by an extended call-cycle over a two-week period. A reminder SMS was also sent in the second week of fieldwork.
16 Taking into account recruitment to the panel, the cumulative response rate for this survey is around 5.0 per cent.