Australian Social Media Data Privacy Report

August, 2020

Almeida Insights

Researchify

About this report

Social media is certainly in the spotlight at the moment. There are concerns about Tik Tok and it's Chinese ownership. In the US, a US Congressional Inquiry is underway into antitrust behaviour from the likes of Facebook and Google (among others). Right here in Australia, the ACCC have commenced proceedings against Google, alleging that consumers were misled about expanded use of personal data. The common thread through these different events is online data privacy.

Closer to home, statements from friends and family like "I have nothing to hide, they can have my data", "who cares if they have your data" and "they don't access anything Alice, you're being paranoid" began to ring alarm bells. In further questioning, it became clear that they didn't care because they didn’t really know or understand what data was being accessed, and for what purpose.

This played on my mind for a few weeks. Did many Australians think this way? Do average Australians know what data is retained and used when they sign up for social media, and more importantly, do they care?

This research is designed to answer these questions and more. My mission is to contribute further to the conversation about data privacy, and perhaps educate Australians so they can make more informed decisions. This is not an attack on social media, but rather an education piece for its users.

If you're reading this, you should care. Your data is far more valuable than you realise, and belongs to you.

I hope you enjoy the report.

Alice

ALICE ALMEIDA
FOUNDER, ALMEIDA INSIGHTS
ALMEIDAINSIGHTS.COM.AU

ALICE ALMEIDA

Founder, Almeida Insights.

Alice has over 18 years experience working in media and marketing research for Australia's largest media brands; Channel Nine, Channel Seven, News Corp, and Fairfax. She has held industry research council positions, was asked to give evidence at a senate inquiry into Public Interest Journalism, and has presented research and data at over 60 conferences locally and internationally.

She has been instrumental in producing market first research pieces and has developed a strong reputation in market as a research and insights leader.

In February 2020, Alice launched her research company Almeida Insights, a full service research consultancy company.

For more information, visit www.almeidainsights.com.au

RESEARCHIFY

Research Partner

Researchify is a market research agency and panel operator that specialises in online panels, community builds and market research consulting.

Researchify has its own online community/panel (What do you think?) of over 100,000 Australians.

They are members of the Australian Market and Social Research Society (AMSRS) and the Association of Market and Social Research Organisations (AMSRO).

For more information, visit www.researchify.com.au

Social Media - Human Behaviour and Privacy

Social media is here to stay. The statistics provided in this report are clear evidence of the popularity of social media platforms, with 99% of respondents subscribed to a social media account and 83% using social media at least daily. It is particularly interesting to see the attitude of users towards their data privacy and security. A popular social media platform was accused of secretly gathering users' data and handing it over to the Chinese government. Since then, this accusation has gained traction, with some countries opting to ban TikTok all together. While there hasn't been any concrete evidence that the alleged data sharing has occurred or continues to occur, a clarion call went out for users to delete the application. However, only 16% of users deigned those reasons as sufficient grounds to delete the app. This trade-off between entertainment and data privacy is not an adequate compelling argument for users to cease their use of social media. It is not easy to alter human behaviour. In fact, a significant and growing percentage of data breaches are attributable to human error. So, what can be done?

Education is always an excellent place to start. Users must be aware of and continuously reminded of the risks to the security and privacy of their data when using social media. Historically privacy has been viewed as an individual issue; however, the networked foundation of social media precludes an individual's control over their data, since others can share a user's information. Research by the University of Adelaide suggests that by analysing the social media posts of just 8 to 9 friends, researchers could predict the behaviour, political affiliations, leisure interests, and personality of an individual with up to 95% accuracy. Additionally, this means if one of your connections is hacked or suffers a data breach, your privacy is at risk.

Users should use unique and complex passwords for each account and implement multi-factor authentication (MFA). Multi-factor authentication requires the user to enter a password, and then another form of credentials, such as a pin sent as a text to your phone or a fingerprint scan. When multi-factor authentication is implemented, it is substantially harder for a cybercriminal to gain access to your accounts and data because they must show they have access to the other authentication factor.

Do not overshare personal information that malicious actors could potentially use to gain access to your accounts, such as birth dates, location, education, and names of pets and family members. Always think twice before posting personal information.

Third-party applications are an ongoing issue due to over-extended permissions granted by inattentive users. Often these third-party applications are not covered under the social media platform's privacy policy.
Before allowing third-party apps access to your account, ensure that the application is not requesting access to more information than is required to perform its function.

Another critical consideration is a user consenting to the use of their data. With 84% of users admitting to not reading the T&Cs before signing up to a social media platform, it is insufficient to have a script at the bottom of abstruse contracts and webpages detailing user's rights to their data and the platform's privacy policy. Informed consent requires easy-to-access and easy-to-read language so the user can acquiesce without having to go to university to study their legal rights.

If we understand our digital profile, where our personal information is located and who has access to it, and implement appropriate privacy and security controls, the privacy risks of social media use can be reduced to an acceptable level. By remaining risk-aware, there is no reason to "unplug" and miss out on the convenience of technology and ease of communication with people and organisations we care about.

Shannon Sedgwick GAICD
Senior Managing Director - Ankura
www.ankura.com

Summary of the findings

With 18 million Australians holding a social media account of some type, and most accessing it multiple times a day, social media should no longer be viewed as entertainment for the young and idle; it's become ubiquitous, and in many cases, undoubtedly an addiction.

The findings of this research have highlighted that there is a significant knowledge gap between what data Australians believe they are giving social media access to, and what is actually being retained and used.

There is also a widespread indifference towards data privacy, ignorance of how personal data is used and monetised, and a pervasive feeling of helplessness in the face of daunting terms & conditions, and convoluted user agreements.

This report highlights that there is much work to be done in educating the population about data privacy. It also raises the question about what else can and should be done to protect users, who currently cannot reasonably be expected to understand and consent to the very things they are being asked to do.

Finally, particular attention should be paid to the repeated themes that emerge from the 18-35 age group, the first generation to spend their formative years in a world saturated with social media. The results that skew heavily towards indifference to the price of social media and data privacy, are alarming not only for them, but for the generations to come, who will know nothing other than this perpetually online world.

The discussion around data privacy has ramped up globally, but this conversation has mainly been from the corporate or government worlds. Now it's time to hear from the users.

How Australians Use Social Media

This section breaks down the usage of Social Media across the various demographics, highlighting not only the breadth of usage (across multiple platforms) but the pervasiveness of this usage in everyday life. We will also look into how Australians engage with the platforms and their motivations for doing so. Finally, we'll touch on the curious case of Tik Tok, which is an illustrative example of Australians' attitudes towards data privacy.

Social media platforms have become embedded in the structure of our daily routines, with 18 million[1] Australians currently holding at least one social media account; that's an incredible 72% of the population. This figure is significant as it gives us a sense of the sheer volume of information that people are handing over, either knowingly or not. We argue that this appreciably raises the stakes in the conversation, elevating data privacy from an issue limited to individual users to one which may require greater engagement and scrutiny from various governing and regulatory bodies.

In our research, we spoke to 2150 everyday Australians over the age of 18, 99% of whom have some form of social media account. In this light, social media should no longer be viewed as entertainment for the young and idle; it's become ubiquitous, and in many cases, undoubtedly an addiction.

[1] WE ARE SOCIAL & HOOTSUITE: THE GLOBAL STATE OF DIGITAL 2020

The power of Facebook in Australia can't be underestimated. It holds a dominant position in this market, reaching 84% of those over the age of 18. The next closest social media networks are YouTube (60%), Messenger (56%), and Instagram (45%). While those under 35 are heavy users of social media across a broad range of brands (80% have a Facebook account, 80% access YouTube, 74% have an Instagram account, and 69% have Messenger), for the other age groups Facebook is by far the primary point of engagement. (Figure 1). This market dominance manifests itself in how people consume news, products, and entertainment, making Facebook a "one-stop shop" for many Australians.

On top of the broad reach among Australians, the other strength of social media is the access rate, which – propelled by the era of smartphones – has seen an astounding rise in recent years. 83% of respondents access social media daily. 61% of those use social media multiple times a day. When this is broken down by age, the numbers shift; 92% of people under the age of 35 access it daily – 79% of those multiple times a day. Compare this with people over 55; 76% access it daily – 46% multiple times a day.

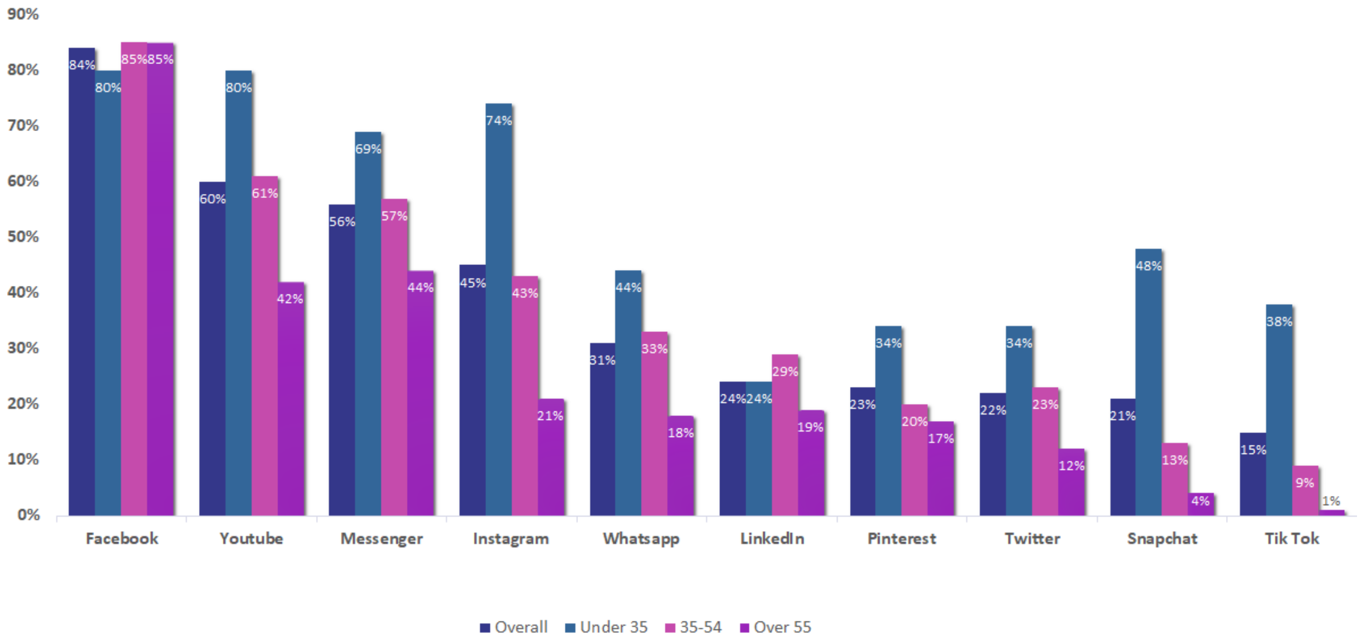


Figure 1: Social Media Usage – by Platform

The high access rate is one thing, but the real value for advertisers on social media is engagement. In this research, we discovered that social media users fall into two groups, that we will call “Publishers” and “Wallflowers”. These groups were determined based on how active they are in sharing on the platform. For example, 76% of Australian’s will post some form of content on social media; 44% of those share content in multiple formats - text, video, and photos, 13% only share text, 12% only share photos and videos, and 7% only use it for direct messaging/instant messaging. (see Figure 2). It’s no surprise that a significant amount of “Publishers” are under the age of 35, whereas "Wallflowers" are more likely to be over 55. Interestingly, over 55s also hold the greatest concern about data privacy (see Figure 3), which may drive their reluctance to engage more actively with the platforms at their disposal.

Reach and engagement (including the access rate), coupled with (as we will see later) a somewhat indifferent attitude towards privacy means that under 35s are the pin-up users for these social media companies. They actively generate the most data, and statistically care the least about what happens to it.

Identifying the reasons why Australians engage with social media is crucial for a couple of reasons. Ostensibly, it allows the service providers to ensure the capabilities of the platform best suit the needs of its users. However it also allows us to appreciate the success of these companies in masking arguably the primary goal of these platforms - data collection.

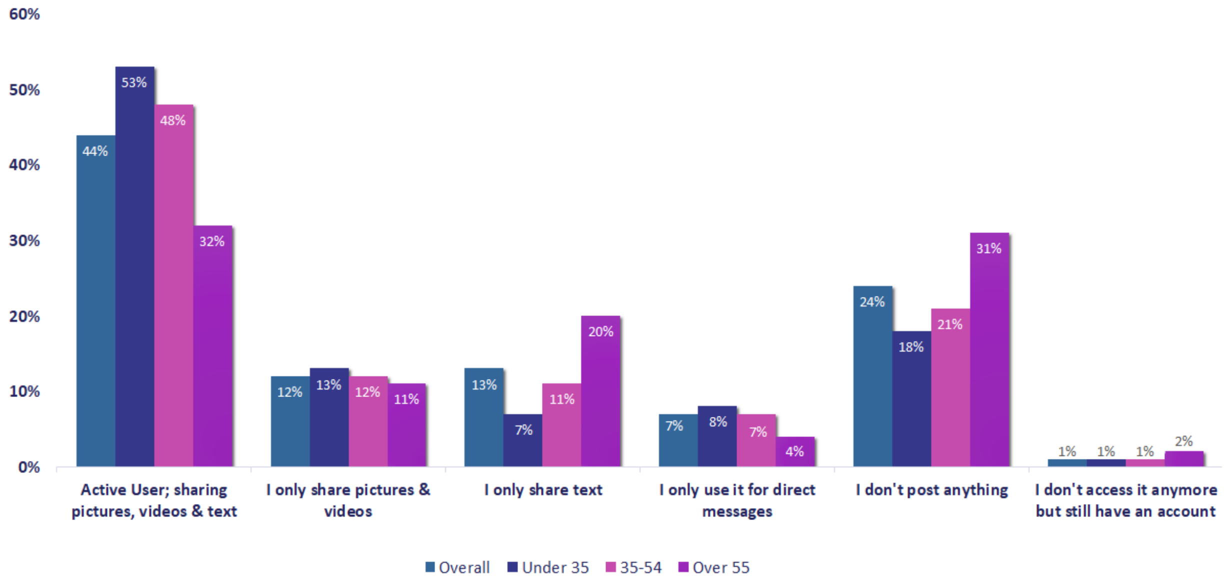


Figure 2: Social Media Engagement

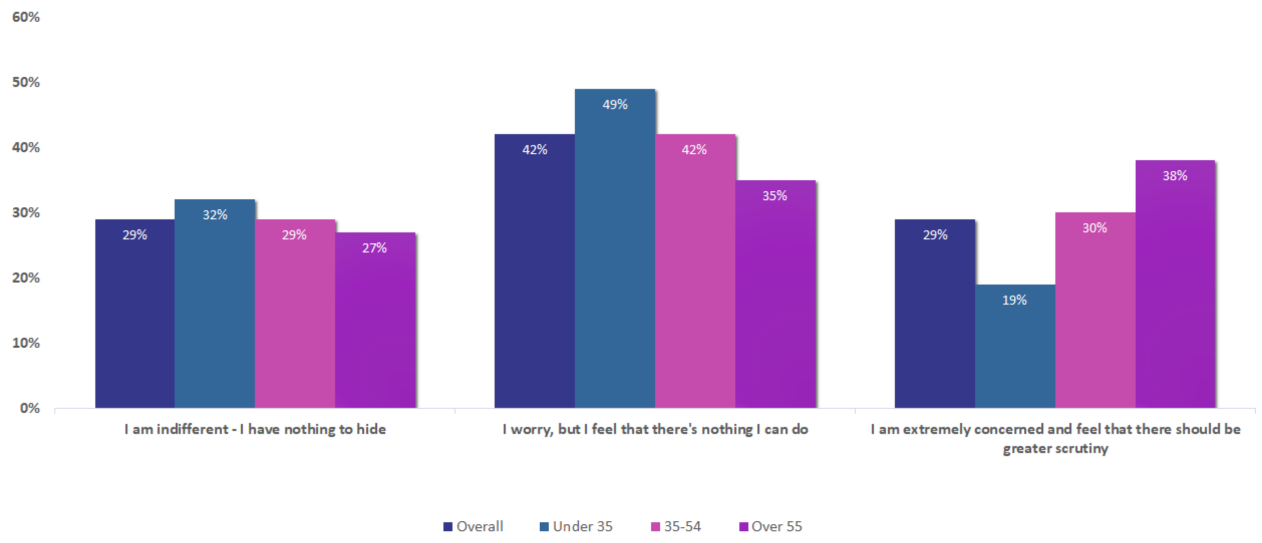


Figure 3: Attitudes to Data Privacy

Unless you operate a postal system or a phone network, keeping people in touch with family and friends is difficult to monetise, yet 64% of Australians indicate that they use social media precisely to keep in touch with family and friends. 70% of those who use social media to stay in touch are over 55, and 49% are aged under 35. It's undeniable that people are using social media as a tool to stay in touch with family and friends. The question it begs is this:

What happens if the primary reason for which you use a service is not the primary reason it exists?

We will explore this further in the next section, and the identified risk of an absence of informed consent.

Tik Tok, the newest social media platform and one of the fastest-growing in the world (aided in part by the COVID-19 lockdown) rose to success not without its share of controversy. In December last year, it was first reported that Tik Tok had been accused of secretly gathering users' data and handing it over to the Chinese government. Since then, this accusation has gained traction, with some countries opting to ban Tik Tok all together. While there hasn't been any concrete evidence that the alleged data sharing occurred or occurs, there are many in the halls of power who believe that the accusation is accurate. When we look at how this may have impacted usage of Tik Tok here in Australia, we see that usage has mainly been negligible.

When asked if they were at all concerned by the alleged connection of Tik Tok and the Chinese government, only 16% cared enough to delete the app (Figure 4) . A further 54% said it made them feel "uneasy", but they would continue to access the app, and a staggering 30% did not care at all. To be clear, this is not because people do not believe the alleged connection exists, but rather because they do not see how the connection – if it exists – affects them.

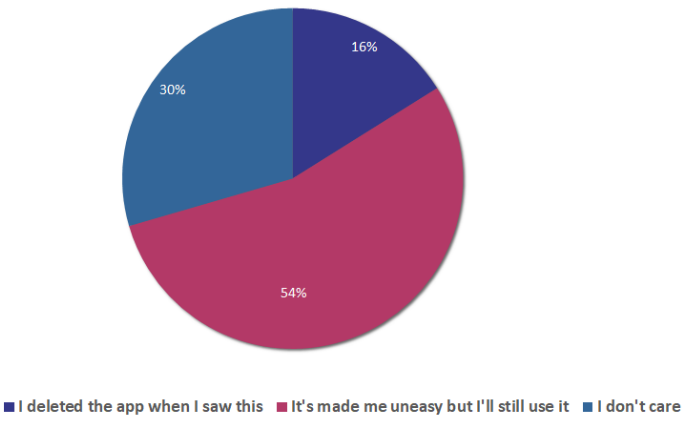


Figure 4: Attitude towards alleged Tik Tok links to Chinese Govt.

Unsurprisingly, 80% of the "don't care" segment is under 35, reinforcing our earlier point about their indifference to data privacy.

What we have seen in this initial component of the research is concerning; social media companies with extensive reach and engagement, users embedding this engagement into their daily lives, a potential lack of understanding of the "contract" between the providers and the users, and a laid-back approach to data privacy. All of these factors combined are worrying, the ramifications of which are discussed in the next sections.

How safe is your data?

While there are numerous ways that data gets captured (and thus potentially compromised if improperly secured), in this report we focus on the five areas below across the social media landscape:

- Primary interactions with the application (eg what you post on Facebook)
- Secondary interactions (eg what websites you visit or access via Facebook)
- Third-Party applications (eg FaceApp, which was provided through Facebook)
- Cybercrime (eg hacking, malware, or stolen data)
- Third-Party access (eg Cambridge Analytica, which was allowed to gather user data without real informed consent, and technology such as the Internet of Things)

We touched on the primary interactions in the previous section. Here we look at the remaining 4 areas.

Social media organisations are some of the largest and most valuable data houses globally. In 2004 when MySpace reached its first million users, and Facebook launched, users were offered a platform to connect, stay in touch, and create an online community. Millions signed up over the years and quite freely gave personal details; insights into how they were feeling, what they liked, what they were doing, who they follow, what interests they have, and so on. All this information was handed over with barely a second thought.

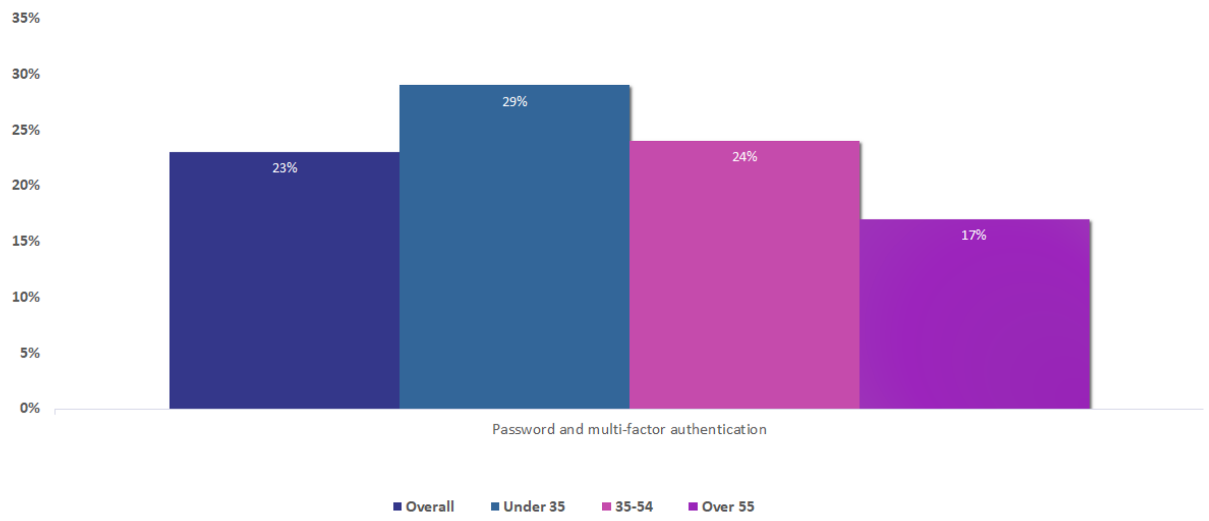


Figure 5: Password & MFA Usage

Accessing websites via platforms such as Facebook or Instagram is just one way in which digital footprint data is captured to build key user insights that assist in targeted advertising and content. Targeted advertising broadly falls under the umbrella of "personalisation" – tailoring the experience to the individual. Relevance in advertising is a key goal for any marketing campaign, and there's no question that this tracking of behaviours greatly assists in achieving that goal. But like the father in Minneapolis in 2012 who found out his teenage daughter was pregnant after Target sent her maternity advertising material, users should continuously be asking:

Who knows, who should know, and why?

The emergence of third-party applications leveraging existing data platforms has made it even harder for consumers to keep track of how their data is being used. FaceApp – through Facebook – gives users an eerie glimpse into the future, a digitally created picture of an elderly version of themselves.

What users may not realise is that it isn't just all of their data on Facebook that this app has access to, but also features like their camera and microphone on their mobile, as well as contacts and other apps. External access requests are listed and managed by detailed Terms & Conditions which the user "agrees" to when downloading the app (see following section), and has become an accepted fact of app usage. With nobody asking why this access is required, the eerie glimpse into the future may be the ever-growing size and scale of this data collection.

If you have a social media presence, attempted cyberattacks are almost impossible to avoid. Only 23% of those surveyed have enabled a multi-factor authentication control measure across their social media (Figure 5). The remaining 77% have not, leaving their social media profile, and the data that goes with it, easily accessible to cybercrime. One example of this was in 2018 where up to 90 million Facebook profiles were hacked, exposing all the users' profile data. To their credit, Facebook reacted quickly, fixing the security breach, and logging out every impacted profile.

Most recently, in July of this year, Twitter was hacked and profiles of users – including some very high-profile accounts, such as Mike Bloomberg, Floyd Mayweather, and Kanye West – were briefly taken over. Tweets were sent out encouraging people to send $1000 Bitcoin, and they would receive $2000 in return. While this attack wasn't large in scale, the hackers still managed to walk away $110,000 USD richer, which still excludes the value of the personal data that they were able to extricate.

These breaches are well publicised. Each time social media experiences a significant attack, it is widely covered on all forms of general media.

It would be near impossible to find someone who isn't aware of social media cyberattacks. Yet that doesn't seem to alter social media usage or behaviour, even for those who have experienced a cyberattack firsthand.

In our research, 20% of all respondents have had their social media hacked in the past 2 years – that's 1 in 5 Australians. To put that figure into context, if 20% of people experienced home or car break-ins, with contents being stolen, it's fair to say we would be living in the midst of a crime wave.

So why isn't personal data held in the same regard as the personal contents in your house? Is it a lack of perceived value or lack of knowledge about what happens to their data once it's stolen? Or both?

The research suggests the latter; a fundamental lack of knowledge on what happens when profiles are hacked (Figure 6). Only 28% believe that hackers accessed their personal information from their profile or device; most believed that they sent spam to their contacts (49%), or posted content on their profiles (38%). While this could have been the case, these outcomes are relatively benign. Personal information is at the core of our digital identity (think security questions for online banking, back up questions for password resets etc.).

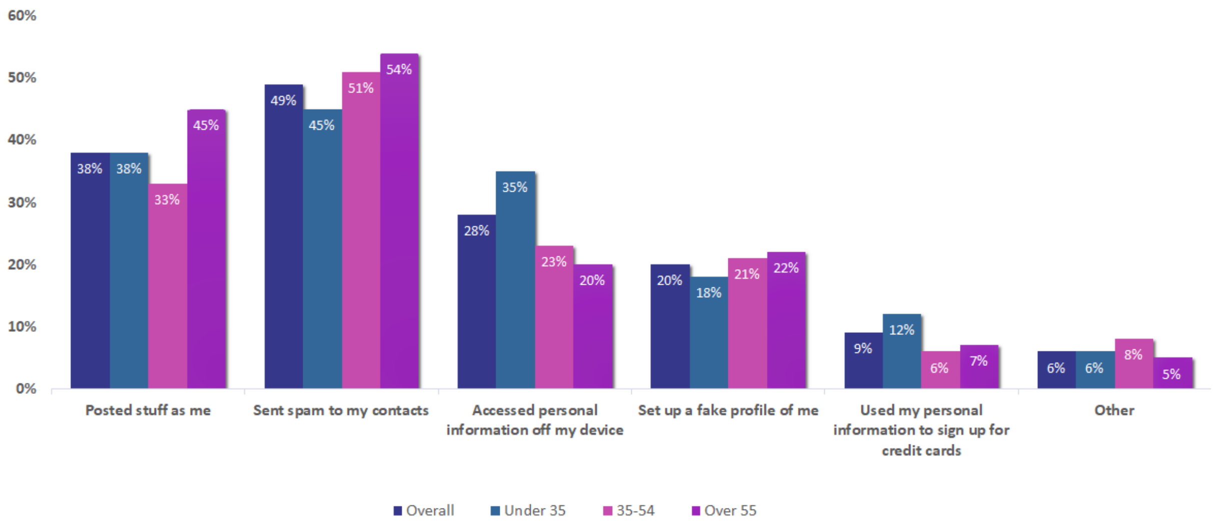


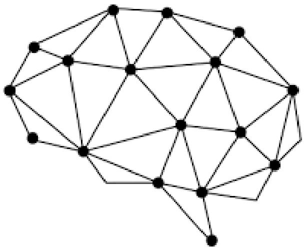
Figure 6: What happens when profiles are hacked?

The loss of this data can result in immeasurable pain for the persons impacted. Yet, the possibility that personal information was accessed during a cyberattack is not considered by 70% of those who are hacked.

Most felt anger (60%), and frustration (47%) of being hacked, however, it seems that these feelings were more directed to the annoyance of being hacked and the delay in accessing their profile - rather than potentially having personal and confidential information stolen. While most profiles were retrieved back relatively quickly (56%), 31% stated it took a while, and 12% didn't get their profiles back.

Whilst there's a definite lack of awareness of the risks of having your data stolen, an alarming finding was that there is also a distinct lack of care for some. When asked how they felt about having their social media account hacked, 1 in 10 Australian's didn't care or felt okay about it.

Their view was that it was an accepted risk of being part of the online community. When delving into this group, 88% of those are under the age of 35 and as we've found throughout this research, this age group is mostly indifferent when it comes to matters of data privacy on social media.



Perhaps the most troubling area is that of Third Party access to personal data. The Cambridge Analytica scandal is the most well-known of these, however, unlike hacks, this issue is far less publicised. In our view, this makes it highly problematic, as users are often unaware of how this data is passed on, used and monetised.

Cambridge Analytica and its sister company Strategic Communications Laboratories, were given access by Facebook to 50 million users’ data and retained it without their consent. This data was then used – among other things – to influence the 2016 US election, which resulted in Donald Trump being elected President. This report is not a commentary on the legitimacy of the election. But take a moment to understand the significance of that event.

Users’ ***virtual activity*** *generated data that was used somewhat surreptitiously to learn about their political leanings. The platform was then leveraged to modify behaviours and actions in the* ***physical world.***

One of the reasons we wanted to conduct this research was to test our hypothesis that the majority of Australians don’t care about data privacy. Regrettably, this was largely backed up in the findings. (see Figure 3)

Only 29% of respondents are extremely concerned about data privacy and feel that there should be greater scrutiny around it. 38% of those are over the age of 55. Our concern lies with those under the age of 35. Almost a third of this age group are ‘indifferent and have nothing to hide’ when it comes to their data. Outside this research, a common sentiment from people within this age group is “they can have my data. Who cares?”.

There is also a group who worry but feel like they can’t do anything about data privacy (42% overall). This result is a concerning stat as it highlights that many believe they don’t have control over their data if they want to participate in social media.

A relatively high rate of breaches and a largely apathetic view of data privacy leads us to believe that a lack of understanding (of both the value of personal data and how it can be used) by Australians may be the key factor in understanding current attitudes. Further, the concept of “lack of control” is borne out in the research in the next section relating to consent, and suggests that people are resigned to the fact that foregoing data privacy is the “cost of doing business” with social media.

We look further at these themes in the next section of the report.

Data Awareness

While a number of the concerns in the previous section are out of the user's control, being mindful of their data and how it's retained and used by social media, is in their hands right from the start. Sure, the easiest way to protect your data is not to participate in social media at all, but ensuring complete safety of your data would also require you never going online again! That's not a realistic option, so the best thing consumers can do is become more aware. It isn't whether you finally agree to hand over your data as the price of engagement. It's whether you know the price, to begin with. It all starts with the initial download and sign-up.

Only 19% of Australian's read Terms & Conditions when downloading an app or signing up for social media, which is troubling (Figure 7). The Terms & Conditions are usually where they list out what data will be captured and where the social media provider will ask for permission to access specific applications and settings on your device.

Over half (53%) of Australian's say they quickly skim over Terms & Conditions and 28% don't read them at all. Instead, they quickly scroll to the bottom and "Accept" without reading a single sentence. Not reading the Terms & Conditions blindly gives apps and organisations access to the most personal information and contents you have; your images, microphone, contacts, and internet history, just to name a few.

Beyond not reading the Terms & Conditions, there also seems to be a level of disconnect between what Australian's think they know, and what they actually know when it comes to how their data is retained and used by social media organisations. For example, 67% of Australian's believe they understand what they agree to in terms of how their data and information is retained and used by a social media provider when signing up.

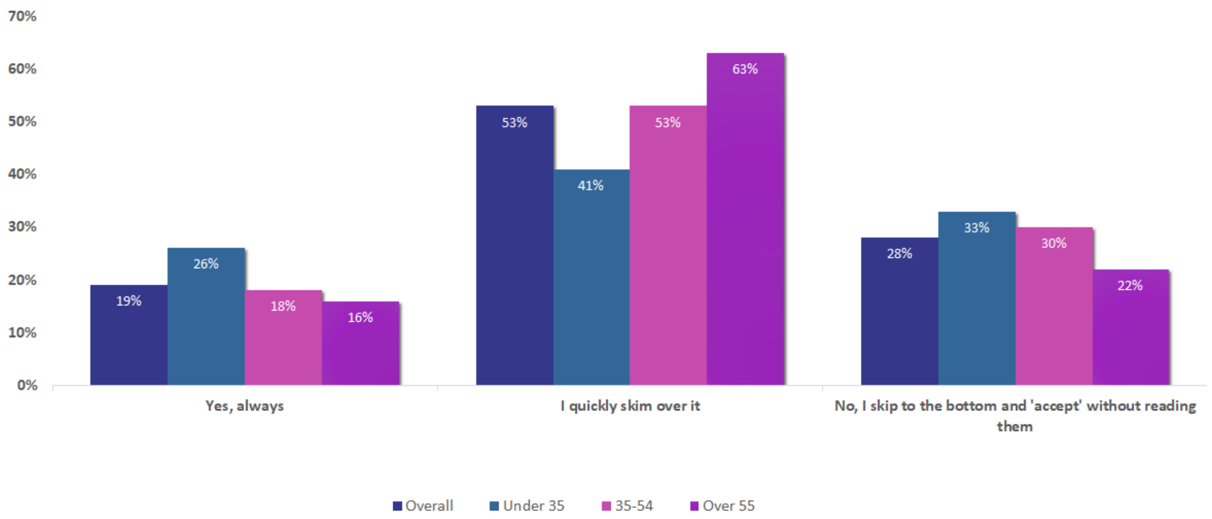


Figure 7: Reading Terms & Conditions

It is difficult to reconcile this with the fact that only 19% read the Terms & Conditions, and the overall knowledge among Australian's of what data is retained and how it is used by social media, is relatively low.

Delving into this further highlights the simplistic understanding that Australians have of what data is being captured and used by social media. When asked what personal information they believe they give access to social media organisations on sign-up, off their device, 64% of users believe it is demographic information such as age and gender. Only a third of respondents believe they give access to device location, media files and photos, and contacts, and 1 in 4 believe they provide access to their camera, microphone, and internet history. The fact that these other access points outside of demographic are relatively low highlights a lack of knowledge of what is actually being accessed.

When asked whether they believe they have a strong understanding of how social media uses their data, only 29% said yes. 65% of respondents 'don't know but feel like they should'. Removing the fact that they could be more aware if they read the Terms & Conditions, this result highlights the knowledge gap between what users believe they agree to, what they give access to, and how social media actually use the data. Understanding the "why" is crucial to informed consent as it clearly explains the impact of making this data available to another party.

A well-informed user may be able to articulate what data they have agreed to hand over, by way of a simple repetition of the warnings or prompts that pop up during the installation of an app.

Without knowing what is being done with this data, they are not in a position to provide informed consent. There is a reason why medical ethics dictate that informed consent is crucial. After all, how can you consent to a procedure which may cause exsanguination* if nobody tells you about the impact?

The most common belief on why social media retains and uses their data is to target them with relevant advertising (69%) and content (41%). These results aren't surprising given nearly all social media captures data to deliver targeted advertising and content. What is alarming though, is that 38% believe that their data is collected to be then sold to another company – for reasons completely unknown. A company selling your data to another company, without your knowledge, should be of huge concern.

When looking at the audience, almost 50% that believe this are over the age of 55. Those aged over 55 are an age group where many are relatively new to social media, have the least knowledge about what social media does with their data, and yet they also believe there needs to be greater scrutiny around data privacy.

As previously mentioned in this report, 42% of respondents worry about data privacy but feel like there's nothing they can do. The fact that a third believe their data is being sold to another company (for reasons unknown) suggests that people have come to a resigned acceptance that their data does not belong to them, and surrendering it is the price of taking their place in the online community.

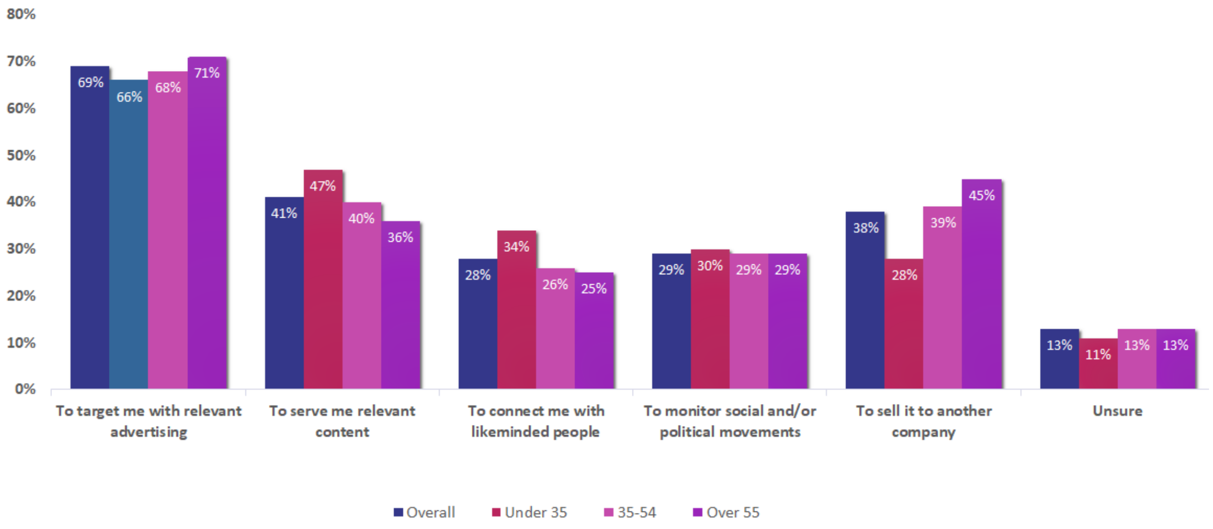


Figure 8: Views on why data is captured

* Loss of blood to a level that will result in death

When we asked Australians about their understanding of what social media costs, 35% said “nothing, advertising pays for it”, and 26% said, “nothing, the app is free”. Only 17% said, “Something, I give them personal information to pay for it”. It is this that is central to the business model for social media, and which seems to be hidden in plain sight.

Generally speaking, social media requires no cash transaction to take place to sign up or download the app. However, to call this “free” is a misnomer. The price you pay is not just the data you hand over, for that in itself has limited value. The way that data is used – to sell, to profile, to tweak, to suggest, to modify – is the price that is paid.

What is interesting is when people were asked whether they believe social media has the ability to influence an individual’s opinions, perspectives and future behaviours, a staggering 79% said yes. This significantly high result suggests that people have a theoretical appreciation for what social media can do, but have not connected this as a value proposition for someone else. Understanding this would mean asking the question:

Is the price that I’m paying the surrendering of my future free choices and independent thoughts, for the benefit of someone else?

Further, only 17% of overall users surveyed indicated that the feeling that their views were being swayed would lead them to reconsider how they use social media. Put another way, of the 79% of Australians who believe that social media can influence future behaviours, 83% do not see this as a compelling reason to question their engagement with the social media platforms.

When asked about social media as a business model, Australian users demonstrated a limited understanding of the role they play. 37%, believe they are a ‘user’; they use the product, and other companies sell things to them through advertising, followed by “I don’t see social media as a business model” (15%) and “I’m the consumer; the company makes the product for me” (14%).

The statistic that over 80% believe social media is paid for by means other than their data and 37% believe their role in the business model of social media is purely as a ‘user’, again highlights the lack of awareness of the value of their data and the power that it gives social media organisations.

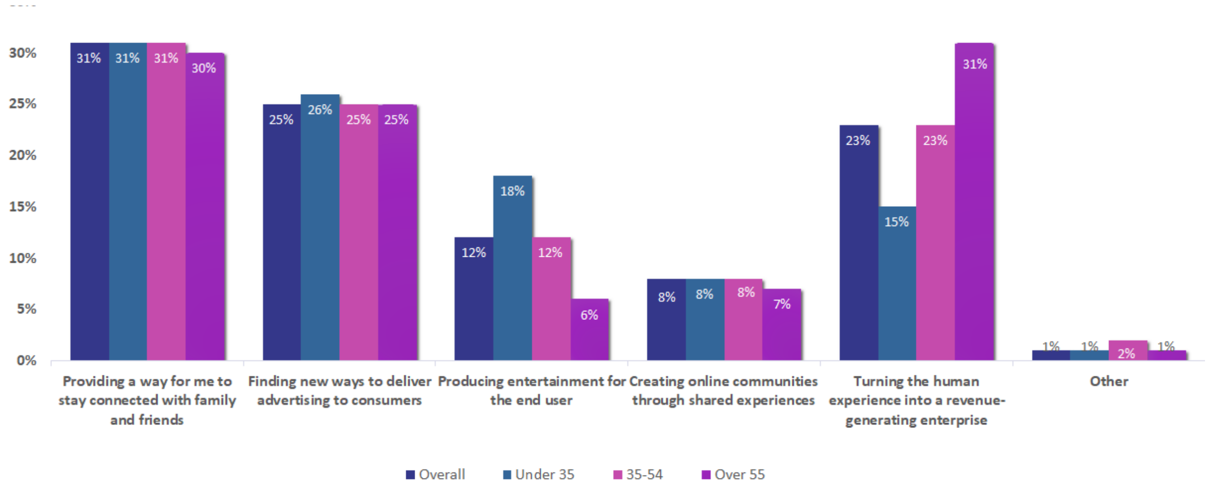


Figure 9: The Goal of Social Media

Social media has been promoted in the market as a place to stay connected and share content. But do Australians see this as the primary goal of social media? According to our findings, only 31% of respondents believe the primary purpose of social media is a communication platform - to provide a way for them to stay connected with family and friends. To revert to the question posed in Section 1, while 64% of people use social media primarily for communication, half this amount believe this is the primary goal of the platform. The next step is for people to question what it means for them, if this is true.

1 in 4 Australians believe that its primary goal is to be an advertising platform, which is finding new ways to deliver advertising to consumers, and 1 in 5 believe that the primary goal for social media is to turn the human experience into a revenue-generating enterprise.

Yes, social media is a great way to stay in touch with those you love (or hate). Yes, it can be great entertainment. And yes, it's become an integral part of our day to day life.

However, our research tells us that Australians are heavily engaged but unaware of the risks and have paid for a product without knowing the price. Social media platforms are expensive to build, maintain, and grow. It's your data that feeds the social media machine.

Afterword

This research isn't designed as an attack on social media organisations. It is designed with the user in mind; the everyday Australian who is active on social media and completely unaware of the value of their data, the risks of exposure, and the use of this data for purposes beyond their purview and understanding. It is designed to build awareness so that they can start to make informed decisions:

What data am I sharing? Who has access to my data? And what are they doing with it?