

The Cost of



Reporting on the State of Digital Identity in 2020

okta

Key Takeaways

1

Consumers underestimate the extent to which their data is being tracked

A significant number of respondents believe companies are not collecting data about their online and offline activities. 39% of Australians do not think online retailers collect data about their purchase history, and 45% do not think their social media posts are being tracked by social media companies. But COVID-19 may be closing the education gap: 96% of Australians are aware of efforts to track the spread of COVID-19 through smartphone data collection, and 29% say the pandemic has made them more aware of data tracking efforts.

2

Consumers say privacy outweighs all, including tracking the spread of COVID-19

While the Australian government and technology companies have launched promising initiatives to track the spread of COVID-19, many consumers aren't buying it. 74% of Australians are worried that data collection for COVID-19 containment will sacrifice too much of their privacy, and 84% of Americans say the same. While 63% of Australians are comfortable with data collection for contact tracing and to determine where the virus is spreading, comfort levels decrease when it comes to using data to track social distancing compliance (34%).

3

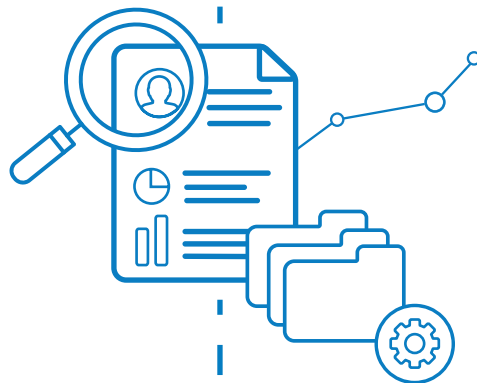
Distrust in government is high

While social media companies are the least trusted overall, global respondents make it clear that governments are still in hot water. 65% of Australians are uncomfortable with the government tracking their data, and only 28% of Australian respondents are willing to share their data to help law enforcement. When it comes to the global pandemic, 30% of Australians say government involvement makes them less comfortable with the idea of data tracking for COVID-19 containment, a concept met with greater discomfort in the US, with 45% of respondents saying the same.

4

Consumers are sitting on gold mines of data, but many won't cash in

We asked global consumers if they'd be more willing to share data with companies if they were financially compensated, and 37% say no. Another 27% are unsure if payment is worth it to sacrifice their data. When it comes to specific types of data, 76% of all respondents are unwilling to sell some portion of their data. Ultimately, consumers value data privacy more than some extra cash.



Introduction

Companies are collecting all kinds of data about our online activities, whether we are browsing the Internet, watching online content, or posting on social media. Together, this record of our data makes up our digital identity. However, there is no official list of what data is collected, leaving consumers confused about where they are being tracked and what data is associated with them. Across the board, people are distrustful and uncomfortable about how their data is being used by companies and governments, even when it comes to noble causes like tracking the spread of COVID-19. Two things are certain: people don't want to be tracked, and they place a high value on privacy.

The unintended ramification is a cost for getting the digital privacy people so badly desire. Data **tracking** benefits companies in many ways, especially those that directly profit from selling consumer data. As a result, consumers often have to sacrifice their privacy to access services they want or need, leading to decreasing levels of **trust**. There is also an unintended tax on citizens' **time** as they struggle to prove their identity repeatedly each year. These "3 Ts" (tracking, trust, and time) reveal the trade-offs that consumers face as they use online services and seek some level of digital privacy.


To better understand how people perceive both their digital identity and how it is managed, Okta commissioned Juniper Research to conduct an online survey of over 12,000 people between the ages of 18 and 75 in six countries: Australia, France, Germany, the Netherlands, the United Kingdom, and the United States. When COVID-19 changed our world, Juniper went back and asked nearly 6,000 of those original respondents how the pandemic has affected the way they think about privacy. The respondents were selected on a nationally representative basis of age, gender, and location. This report will summarise the findings of that survey.

A digital identity crisis: Consumers have a fuzzy vision of their online presence

Privacy has become a hot button issue over the last few years as consumers worry about who collects, stores, and uses their personal information. But exactly what personal data is being collected? Most consumers vastly underestimated the breadth of data used by companies to identify individuals online.

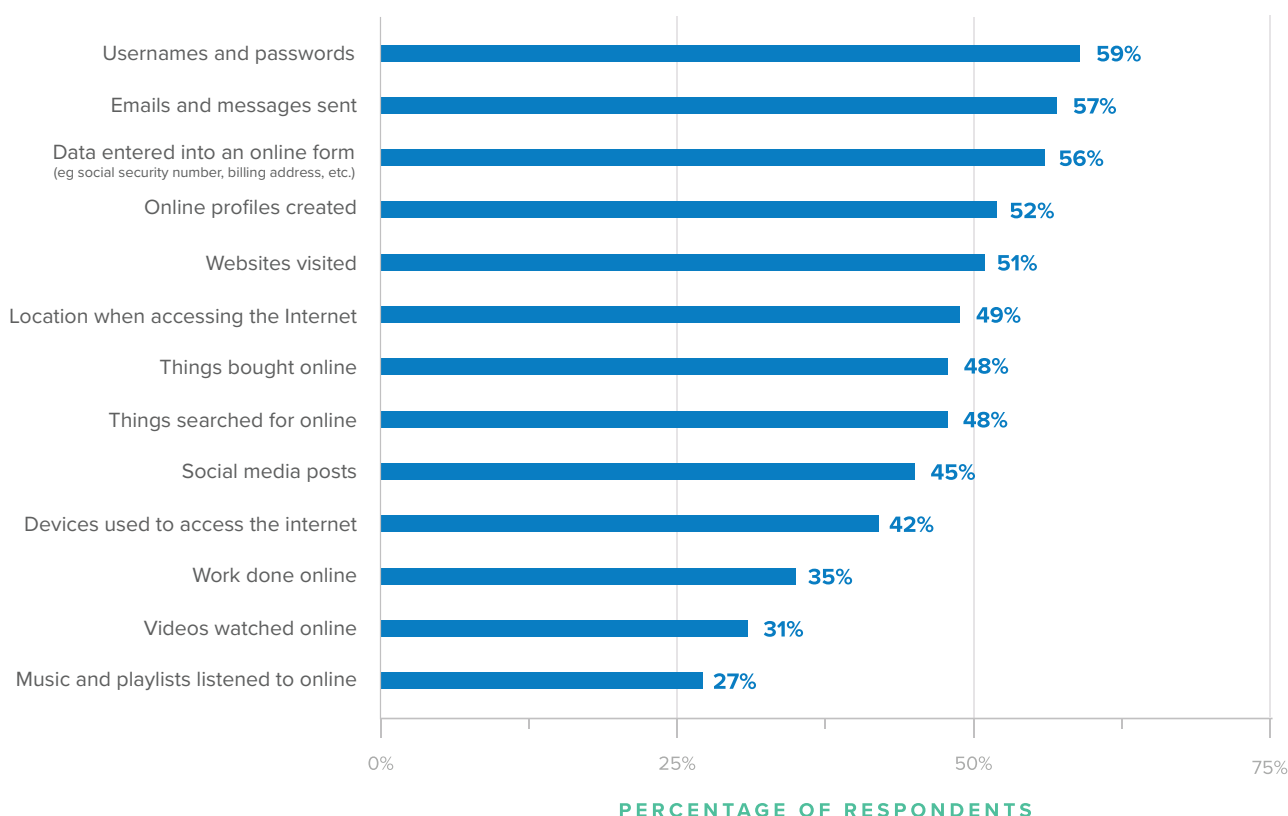
Consumers have significant blind spots when looking at their digital identities

When looking at a list of 13 different types of commonly tracked online data — such as usernames, browsing history, and social media posts — the average survey respondent believes only 6 of these types of data constitute their online identity. This number is higher in Australia, with respondents believing an average of 7 types of data make up their digital identities. In France, this number drops to 5, demonstrating the lowest understanding.



On average, Australian consumers believe 7 types of data make up their online identity

What do global consumers consider to be part of their online identity?



News flash: women and boomers are more identity-conscious

Women are consistently more aware of the types of data that are contributing to their online identities than men.

For example, Australian women are 7 percentage points more likely to think their social media posts are a part of their online identity. 59% of them believe data entered into a form, such as a Social Security number, birthdate, or billing address, is associated with their identity, compared to 56% of men. And when it comes to music and playlists you listen to online, 33% of Australian women think it counts toward their digital identity compared to only 27% of men.

The same can be said of older generations. Australian respondents between the ages of 25-34 say an average of 6 types of data contribute to their online identities, in contrast to those aged 55-64 who average 8 types of data. Other countries surveyed showed similar trends.

Is ignorance bliss? Consumers underestimate the extent to which their data is being tracked

There is a common expression that says, “if you’re not paying for the product, you are the product.”¹ The Internet provides a wealth of information and services that consumers now think of as “free,” but they often forget that their “free” email address, Internet search, and social media account are being funded by advertising dollars, and those advertisers are buying access to them, the end user.

From Cambridge Analytica to the news that Australia’s My Health Record has suffered two potential data breaches, a never-ending list of controversies have shed a light on consumers’ shrinking levels of privacy. Yet, our data shows that many consumers are not aware of the routine tracking and data harvesting that takes place daily.

Dance like no one is watching... or listening

A significant number of respondents believe their online and offline activities are not being tracked. More than 3 out of 4 Australian respondents (77%) don’t think a consumer hardware provider such as Apple, Fitbit, or Amazon is tracking their biometric data, and 52% say the same about location data. 73% of Australians don’t believe streaming services are collecting information about their online media consumption, and 80% don’t think their broadband provider does either.

¹ Scott Goodson. “If You’re Not Paying For It, You Become The Product.” *Forbes* (2012): <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#3c8f06135d6e>

Online communications are also presumed to be private by a surprising number of respondents. Nearly half of Australian respondents (49%) don't think email providers are tracking their email and messaging history, and 74% say the same of their employer.



39%

of Australians don't think online retailers collect data about their purchase history.



27%

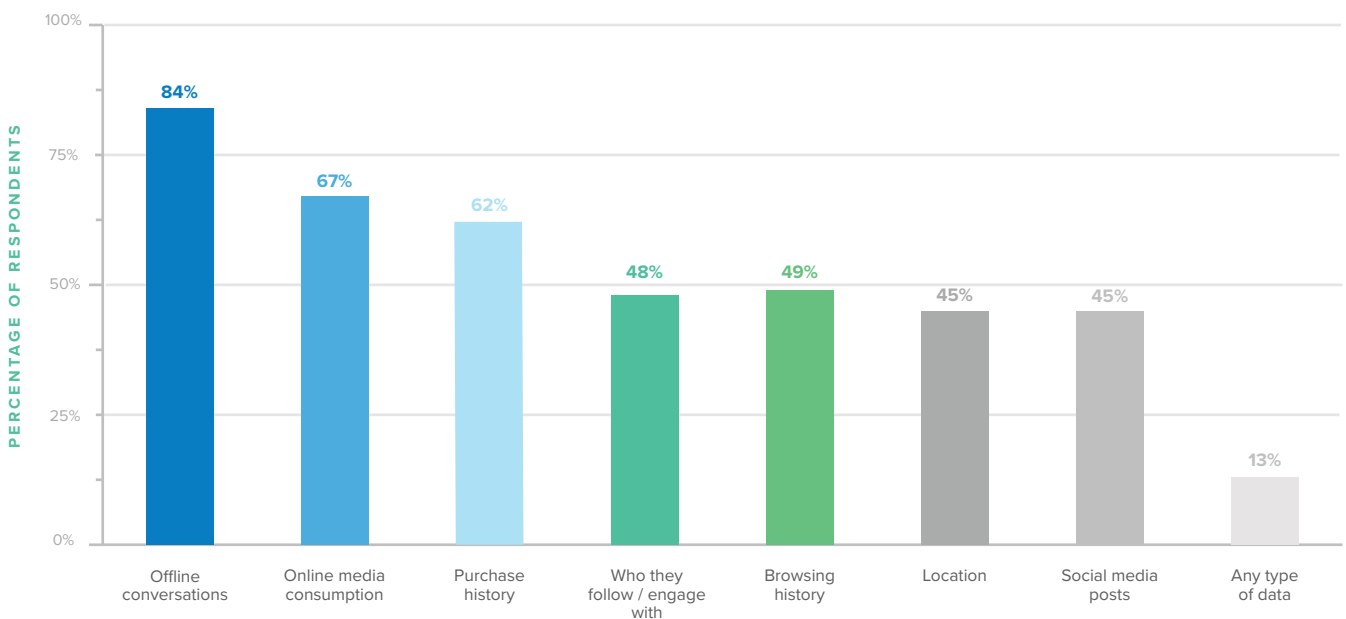
of Australians don't think search engines collect data about their browsing history.

Despite the bad press, many consumers aren't aware of social media tracking

As consumers scroll through their feeds, they have a general awareness that social media companies are tracking something: over 80% of respondents in all markets believe that social media companies are tracking at least one element of their data.

Respondents from the Netherlands are the most likely to expect a social media company to actively collect data on their social media posts: only 40% do not think this data collection is occurring. In contrast, 59% of French respondents do not think their posts are being tracked by social media companies, and 45% of Australians agree.

What Australians do **not** believe social media companies are collecting



Tracking a pandemic

In 2020, people have been inundated with COVID-19 news, consuming constant updates about case counts, reopening plans, and potential strategies for fighting the pandemic. So much so that just 4% of Australians are unaware of efforts to track the spread of COVID-19 through smartphone data collection. Australians are far more informed than respondents in other countries. 14% of Dutch respondents, 17% of Germans, and 35% of Americans are unaware of data tracking efforts to contain the novel coronavirus.



19%

of Australians are more opposed to data tracking in the wake of COVID-19

Still, COVID-19 may be closing the data tracking education gap: more than 1 in 4 Australians say the pandemic has made them more aware of data tracking efforts (29%) as well as the possible benefits of data tracking (29%). In the UK, 32% and 31% of respondents say the same, respectively.

Distrust and discomfort in the age of COVID-19

Whether or not consumers understand what is being tracked, they are generally unhappy that companies are tracking their data, regardless of why it's being collected. Across all countries surveyed, 91% of consumers are uncomfortable with at least one kind of organisation tracking their data.

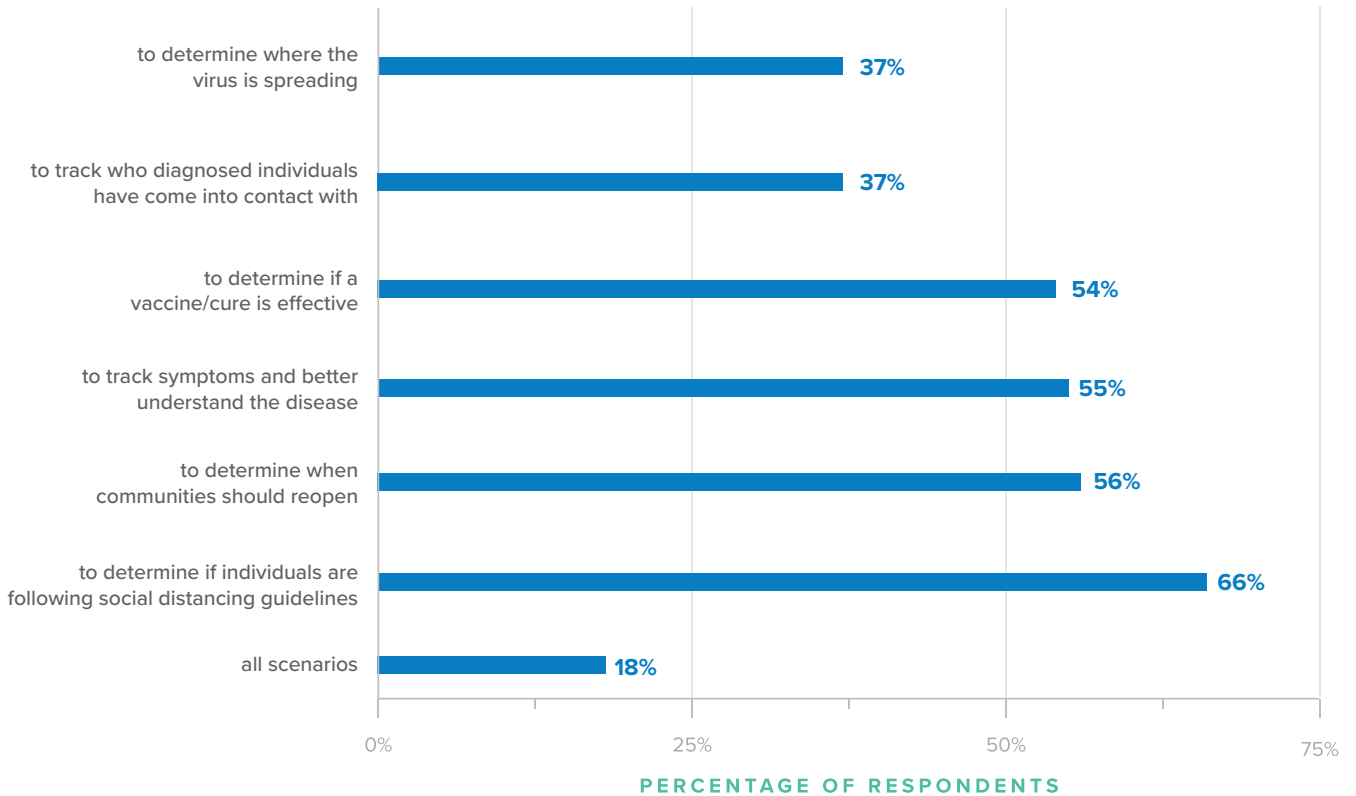
Though if there's ever been a time to justify the sacrifice of digital privacy, COVID-19 is it. While the Australian government and companies like Apple and Google are making a concerted effort to safeguard consumer privacy while tracking the spread of the virus, respondents still feel uncertain about the potential privacy and security ramifications.

Freedom over everything: Australians won't give up their data to slow the spread of COVID-19

Australians show widespread discomfort with the idea of their data being collected to aid the containment of COVID-19. A majority of Australians say they are uncomfortable with personally identifiable information (60%), bluetooth data (53%), and location data (51%) being collected. Australians are slightly more comfortable with medical data (46%) being collected for this purpose. Consistently, older Australian respondents (ages 55-75) are more comfortable with the idea of data collection to track the virus than younger respondents.

In the UK, respondents are far more willing to sacrifice their data to stop the pandemic. Only 51% are uncomfortable with their personally identifiable information, 43% with their bluetooth data, 40% with their location data, and 39% with their medical data being collected.

When Australians are **uncomfortable** with their data being used in relation to COVID-19



Across all countries, discomfort levels rise when asked about data being used in scenarios that regulate individual behaviour, such as enforcing social distancing or determining when communities should reopen.

Privacy and security concerns swell during COVID-19

While the public health benefits of collecting data to track the spread of COVID-19 are clear, consumers in every country surveyed are worried about privacy. A whopping 74% of Australians worry they will be giving up too much of their privacy, and 81% of Germans and 84% of Americans agree. Security is another looming concern, with worrying that data collection for COVID-19 will make their data insecure. This is an even bigger concern in the Netherlands, where 90% express concern.

Trust, or lack thereof, is a big part of the problem. 79% of Australians worry their data will be used for purposes other than COVID-19. This was the number one concern in Germany (87%), the US (86%), and the UK (84%).

Why are Australians worried about data collection for COVID-19 containment?

61%

worry it will impact their finances (e.g. insurance premiums, medical bills)

63%

worry law enforcement will access their data

73%

worry their data will be used to serve advertisements to them

We asked what could be done to make consumers feel more comfortable with their data being tracked for COVID-19 containment, but a consensus couldn't be reached. 23% of Australians say nothing can be done to make them feel more comfortable, with 30% of Americans saying the same - the highest of any country. 53% of Australians say a limit on who can access the data would do the trick. Other solutions include: needing to give explicit consent (39%), putting a limit on how long the data can be tracked (47%), making sure data isn't shared with organisations outside of Australia (48%).

While it is clear that privacy is a concern, the root of the problem may be uncertainty around whether smartphone-based data collection is an effective way to slow the pandemic. 54% of Americans said they believe it is not effective, and only 10% believe it is very effective. Australians are the most optimistic, with 62% believing in the efficacy of smartphone tracking.

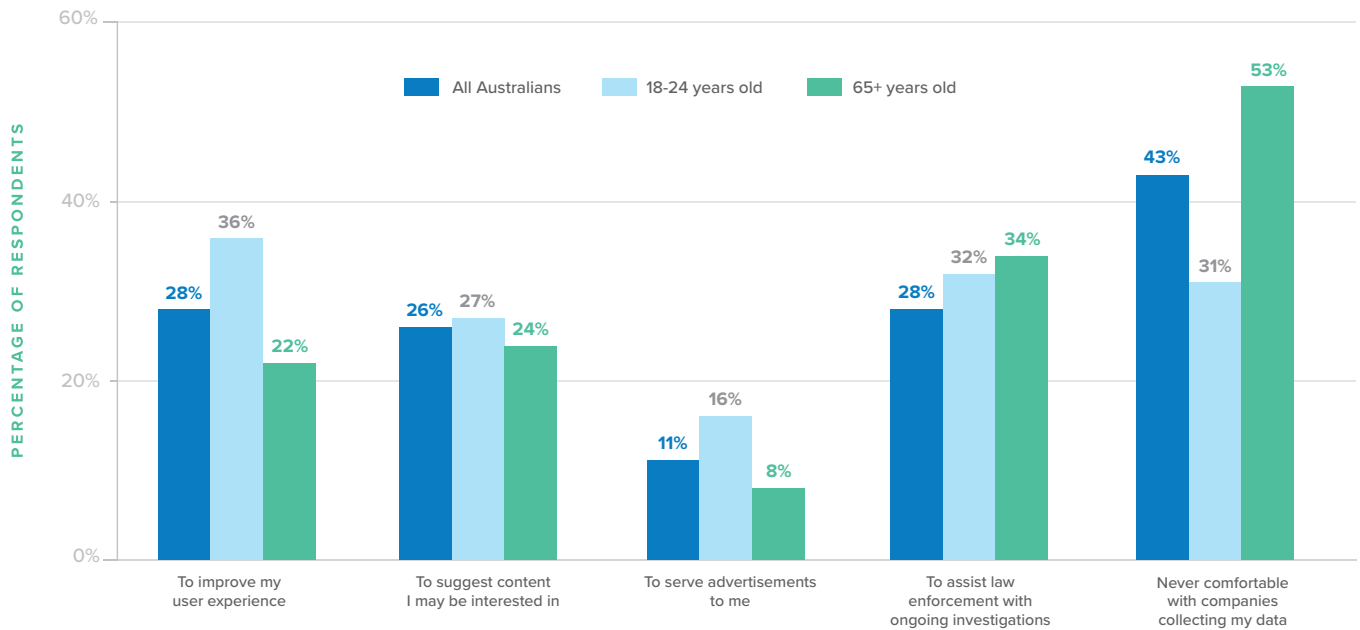
Never say never: some consumers see benefits of data collection

28% of global respondents say COVID-19 has made them more open to the possible benefits of data tracking. But even before the pandemic hit, over half of all respondents were amenable to some form of data collection in exchange for personal and community benefits.

Across the board, Australians aged between 18-34 are likely to be more comfortable with data collection if it results in some type of personal benefit, whether that be an improved user experience (36%) or relevant content (28%).

Overall, global consumers are not likely to share their data to help law enforcement. The vast majority of respondents don't think the benefit is worth the cost, despite conversations about how facial recognition technology and genetic data can aid police investigations. Consumers in the Netherlands are the most willing to share their data to help law enforcement, at 31%. Just 28% of Australians are willing, with only 24% of Americans and 22% of Germans saying the same.

Reasons Australian consumers are comfortable with companies collecting their data



Not all data is created equal

Respondents across every country make it clear that protecting their privacy is a priority, but of course, they consider some types of data more valuable than others.

In Australia, more than 80% of respondents are uncomfortable with sharing any type of data. Respondents are the least concerned about organisations tracking their purchase history and online media consumption, with 80% expressing concern. Biometric data, passwords, and offline conversations are all top concerns.

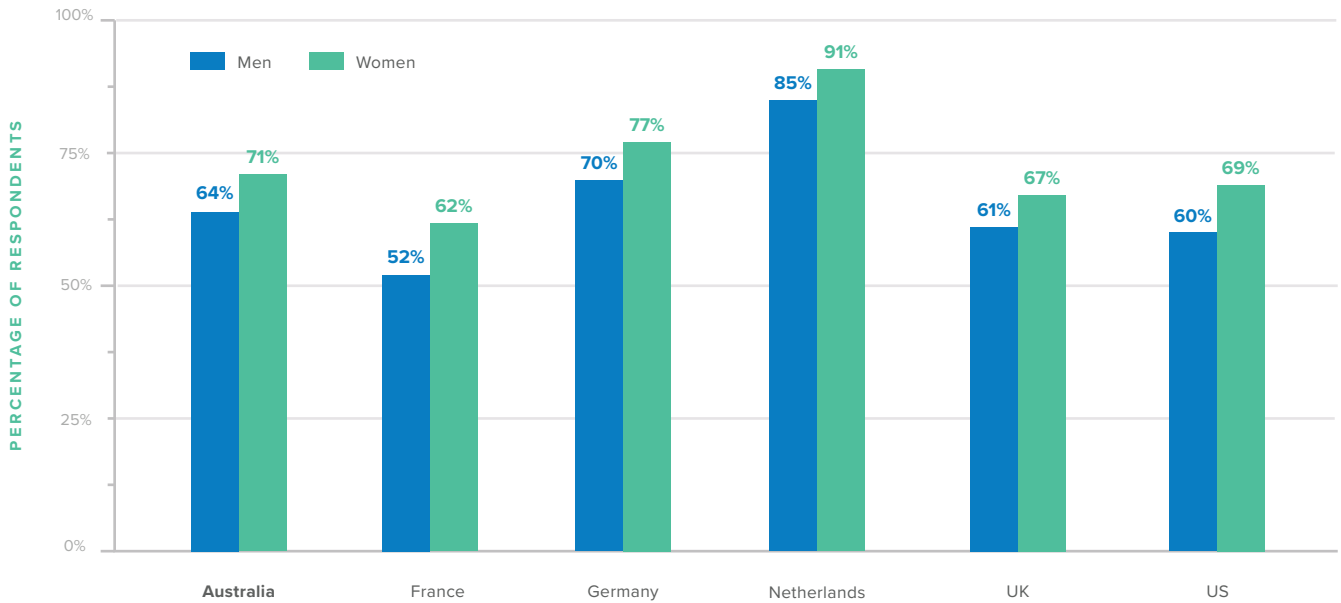
Location, location, location: consumers dislike location tracking

Location data is the most common type of data that global consumers think companies are tracking, yet at least 57% are uncomfortable with their location being tracked. Consumers see buzzy articles about how to correctly set the privacy settings on smartphones, but those can give a false sense of security: Google was exposed for storing location data on smartphones even if the consumer had used a privacy setting that said it would prevent Google from doing so.²

In Australia, 82% of respondents are uncomfortable with their location data being collected. Across all countries surveyed, an interesting trend emerges: women are between 6-10 percentage points more uncomfortable with the issue than their male counterparts.

² Ryan Nakashima, "Google Tracks your Movements, Like it or Not," Associated Press (2018): <https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not>

Discomfort with location data collection



Protecting “real life” data

Almost half of all respondents believe their offline conversations and biometric data are being tracked by at least one kind of company online, although there is little consensus as to which kinds of companies are engaging in the data collection. Respondents in the Netherlands show the highest rate of discomfort, with 90% saying they are uncomfortable with offline conversation tracking, and 88% are uncomfortable with biometric data collection.



Offline conversations

40% of Australians believe their offline conversations are tracked by at least one type of company. Of this group, **83%** are uncomfortable with it



Biometric data

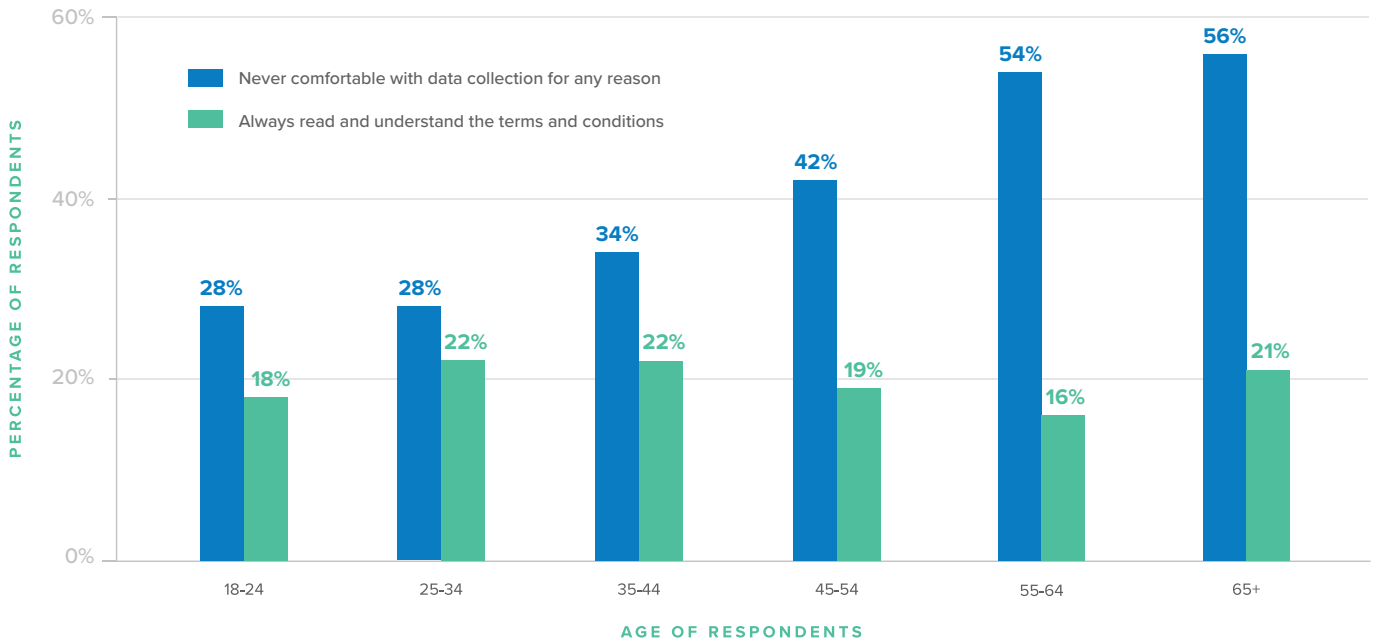
89% of Australians believe their biometric data is tracked by at least one type of company of this group, **81%** are uncomfortable with it

Older and wiser, or just not interested in the fine print?

Data collection sentiments are directly linked to the age of the respondents. 43% of Australians are never comfortable with any form of data collection for any reason, but when broken out by age, the difference is striking. Of respondents ages 18-24, 31% are never comfortable with data collection, compared to 53% of respondents ages 65 and up. This disparity between generations is consistent across all countries surveyed.

One explanation is that younger respondents are more likely to take the time to educate themselves about the uses of their data. In Australia, only 20% of respondents always read and understand the terms and conditions of a digital services website.

Percentage of Australians who are never comfortable with data collection for any reason, compared to percentage of Australians who always read and understand the terms and conditions



Crossing the line: consumers don't want companies profiting off their data

Compared to data collection, an even bigger concern for a majority of consumers is that companies are **profiting** from their data. 93% of all respondents are uncomfortable with companies selling some portion of their data, and 67% are uncomfortable with any form of their data being sold.

More than nine out of 10 Australians (94%) are uncomfortable with companies profiting from at least one type of their data. The sale of biometric data, passwords, and offline conversations cause the most concern at 86% each. Purchase history and online media consumption are of the lowest concern, but 80% of Australians still report being uncomfortable with companies selling this data.

A trust problem: Does it matter *who* is tracking?

The answer is yes: it matters who is tracking your data. Although 46% of all respondents are uncomfortable with data tracking in any form, consumers in all countries surveyed have varying comfort levels depending on what type of organisation is collecting the data.

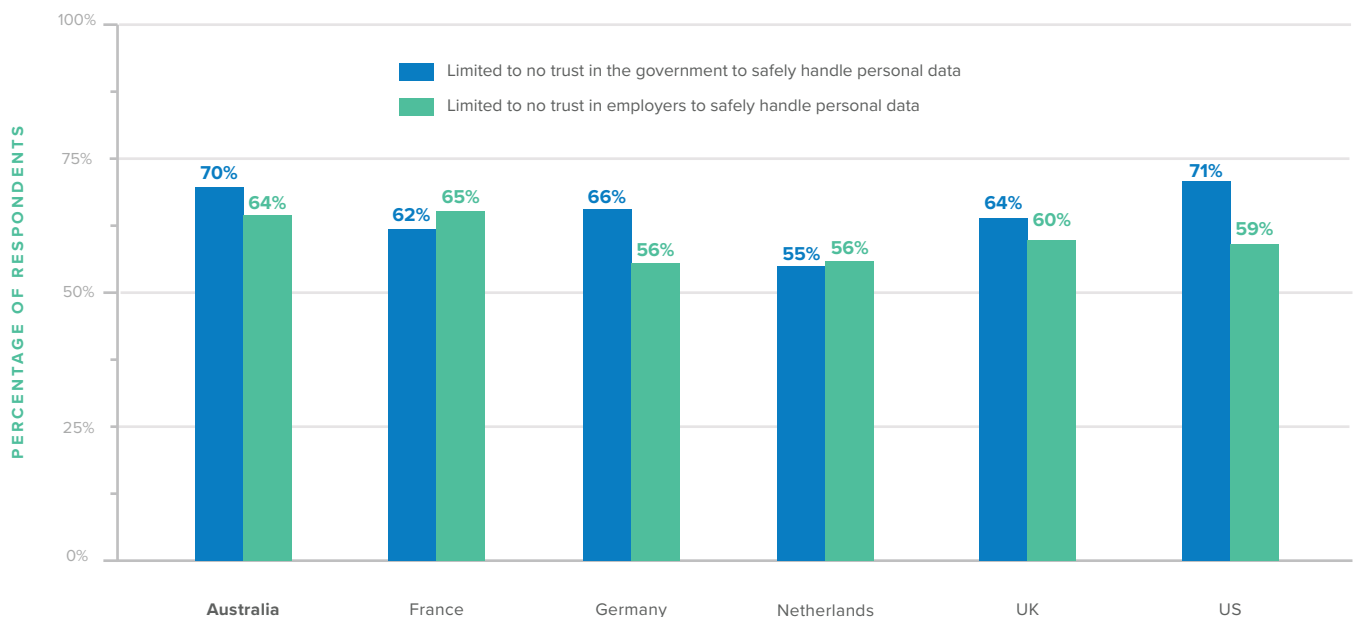
Distrust in government: big brother is watching

The idea that the government tracks consumer data is a big concern for all respondents, especially in the US (70%), Netherlands (73%), and Germany (74%).

In Australia, trust in the government's ability to safely handle personal data is particularly low, with 70% saying they have limited to no trust in the government's ability to do so. When you break down the respondents by age, a clear divide emerges. 41% of Australians aged 25-34 have trust in the government's ability to safely handle their personal data, while only 25% of Australians aged over 55 feel the same way.

In the US, UK, Australia, and Germany respondents report significantly higher trust in their workplace to handle their personal data than the government.

Consumers with limited to no trust in their government or employers to handle their personal data



Survey respondents also believe the government is the most likely group to collect their biometric data and offline conversations. Social media companies and search engines take a fairly distant second and third, respectively.



20%

of Australians think the government collects data about their offline conversations



28%

of Australians think the government collects biometric data about them, surpassed by America at 29% and Germany at 31%

Trust and leadership during COVID-19

Outside of the US, survey respondents are largely happy with how their government is responding to COVID-19. In Australia, 87% think their government's response has been effective. 84% in the Netherlands, 80% in Germany, and 65% in the UK say the same. Meanwhile, only 49% of American and 53% of French respondents think the government has effectively responded to the pandemic.

While the vast majority of Australians think their government's response to the pandemic has been effective, 30% say government involvement makes them less comfortable with the idea of data tracking for COVID-19 containment. Americans are the least comfortable at 45%, with respondents in other countries falling between 26% and 34% when asked the same question.



22%

of Australians would feel less comfortable with the idea of data collection for COVID-19 if healthcare companies were involved



38%

of Australians would feel less comfortable with the idea of data collection for COVID-19 if law enforcement was involved

However, trust in the technology industry is even lower, with social media companies being the worst off. 63% of Australians say they would feel less comfortable with data tracking for COVID-19 if social media companies were involved; many say the same of technology startups (57%) and large and established technology companies (53%).

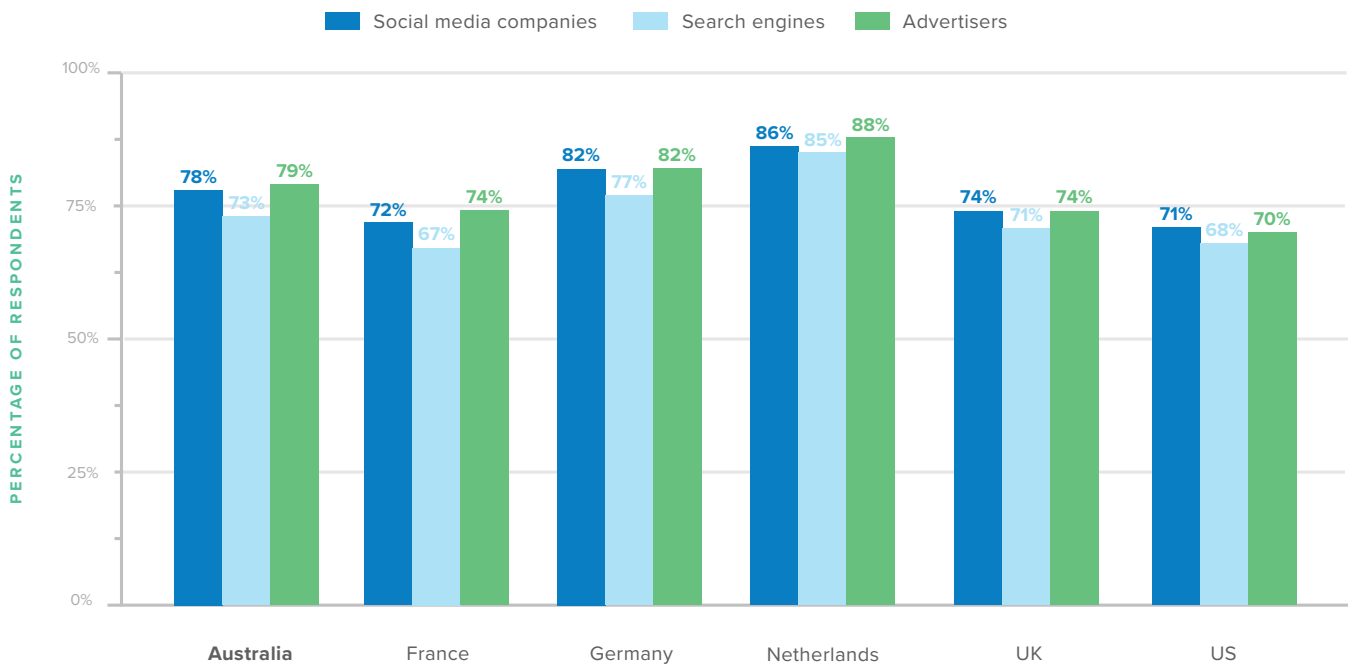
Distrust of social media providers: who watches our Facebook posts more closely, our friends... or Facebook?

Consumer distrust of data collection by social media companies and advertisers is particularly high, which is problematic considering they're involved in the majority of third party data sharing online. High-profile accusations against social media companies and advertisers likely contribute to this level of distrust.

Across countries surveyed, respondents who think social media companies track more aspects of their data are more uncomfortable with social media companies collecting their data. Australian respondents think social media companies track an average of 5 types of data, and 78% are uncomfortable with it. In the Netherlands, respondents are the least trusting of social media companies, believing they track an average of 6 types of data, with 86% uncomfortable with it.

When it comes to data collection, mistrust of social media closely parallels mistrust of advertisers and search engines.

Consumers' discomfort with social media companies, search engines, and advertisers collecting their data



A new economic model? Some say data could be the new property right, but not so fast

Tech companies typically own the data that is generated by users on their platforms. But in order to give consumers more control over the collection and sale of their data, some academics and politicians have proposed the idea that organisations should pay consumers for access to their data. American author and law professor Eric Poser suggested that “big tech companies would get better data if they paid people with money for their specific contributions.”³ At first blush, this sounds appealing, but our data shows that consumers aren’t buying it.

30%

of all respondents are unwilling to sell any type of data for any price

15%

of respondents age 18-24 are unwilling to sell any type of data

48%

of all respondents ages 65+ are unwilling to sell any type of data

“Data for dollars:” compensation isn’t enough

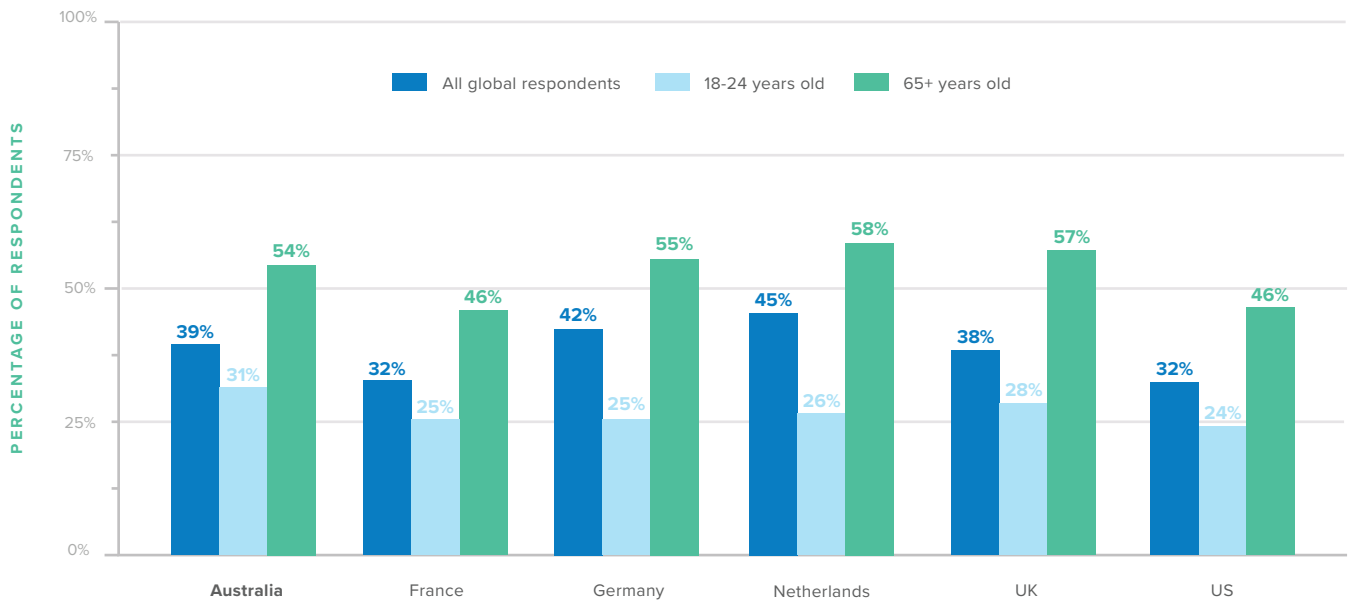
We asked global consumers if they’d be more willing to share data with companies if they were financially compensated, and 37% say no. Another 27% are unsure if payment is worth it to sacrifice their data. When it comes to specific types of data, 76% of all respondents are unwilling to sell at least one type of their data at any price. Ultimately, consumers value data privacy more than some extra cash.

Breaking out the results by country, Dutch and German consumers are the least likely to be incentivised to share their data for compensation, with 45% of Dutch consumers and 42% of German consumers unwilling to sell. American and French respondents are the most open to the idea, but still show hesitations. Nearly 1 in 3 respondents from the US and France (32%) do not find the idea appealing, and another 26% and 27% respectively say they are unsure. Australians sit in the middle, with 39% unwilling to sell their data.

The biggest divergence in opinion can be seen by age. Younger generations are far more willing to share their data at a price.

³ ON CULTURAL MONOPSONIES AND DATA-AS-LABOR, Poser 2018: <http://ericposner.com/on-cultural-monopsonies-and-data-as-labor/>

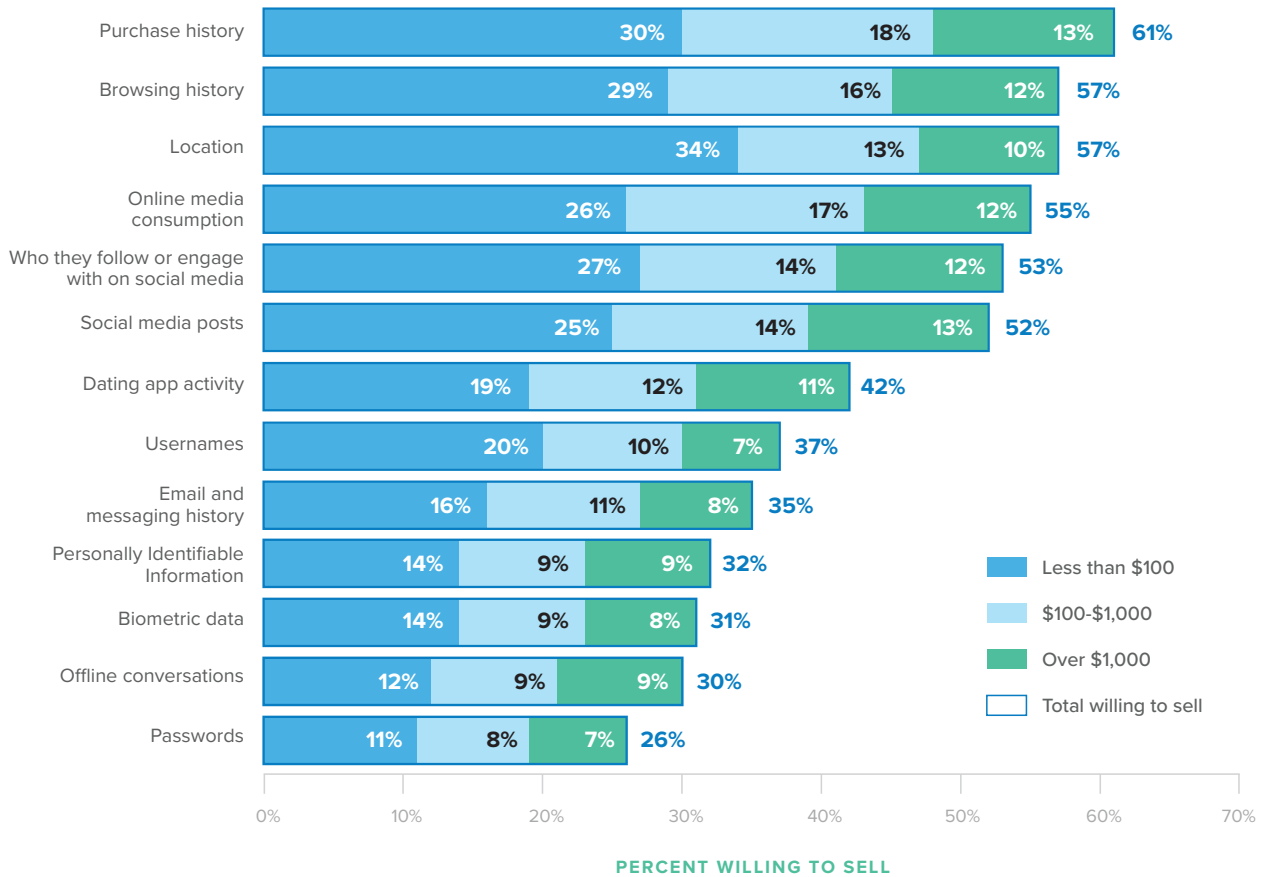
Consumers unwilling to share data with companies for financial compensation



Of course, everything has a price. We asked consumers if they'd rather sell their data or give it away for free, and more than 90% in all countries surveyed say they would take the cash. But data doesn't come cheap. For example, 31% of Australians want \$100 or more for a company to access their purchase history. 23% want that same price for their location data.

These price tags don't bode well for companies trying to make a policy like this work. Facebook, for example, has 2.5 billion users. Paying each of those users \$100 in exchange for their location data — not to mention their purchase history, browsing history, etc. — comes out to a whopping \$250 billion. This economic model would be even less effective for small businesses who need user data to improve their product but don't have the resources to pay for it.

Data Australians are willing to sell and at what price



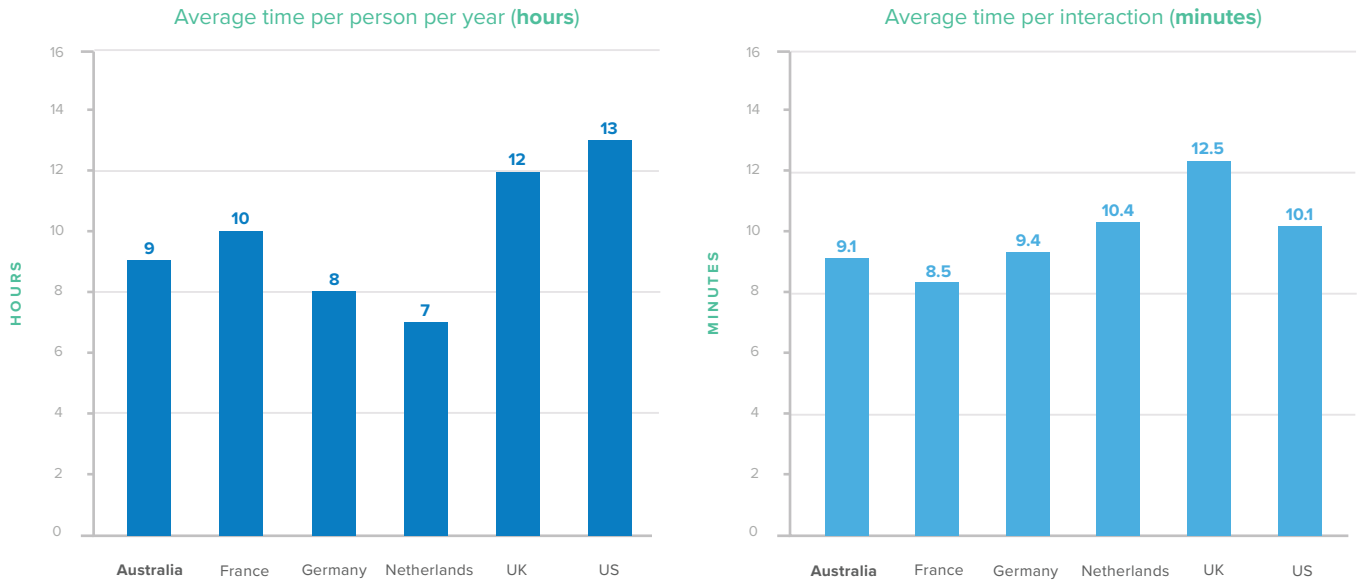
Identity verification is taking a toll on democracy

As governments try to reduce cost and improve accessibility, they are increasingly making services available online. Of course, verifying the identity of a visitor is a critical issue when providing access to government records and services. But there is a trade-off between security and usability: if the barrier to entry becomes too high, citizens will abandon the process, and possibly give up on the service entirely.

Streamlined online access can free up hours of time

We asked respondents in each country surveyed how long they spend logging in or otherwise proving their identity with a variety of government departments, and on average, they're spending 12 hours per year. When looking at individual countries, the number ranges from 7 in the Netherlands, to 13 in the US.

Amount of time consumers spend proving their identity to government departments



The relatively low amount of time each French person spends interacting with different government departments can likely be attributed to the unified Service-Public.fr identity portal. This allows a wide range of functions to be carried out through a single interface. The average French person spends just over 10 hours per year proving their identity, a 26% improvement over the US. Australia has consolidated some government services within the MyGov portal, with Australians spending on average 9 hours per year proving their identity.

Implementation of unified identity solutions can save a large amount of time for both governments and the public they serve; if the US achieved the same level of efficiency as France, for example, its population would save nearly 19 million days.

Conclusion

As our lives migrate to the digital realm, our online identity has evolved to become an increasingly robust collection of data about every aspect of our online and offline lives. This data is extremely appealing to companies and governments who wish to use it for a variety of purposes.

Our survey suggests that consumers around the world have only a vague understanding of how much of their data is being tracked, where, when, and by which organisations. But despite this lack of awareness, they're largely uncomfortable with the idea of companies collecting and selling their data, even when it comes to benevolent causes like tracking the spread of the COVID-19 pandemic.

Okta believes it is important to balance privacy and innovation. Consumers deserve to have control over their data, but at the same time, data is often essential to building new technologies and serving the common good. To strike a balance, organisations around the globe must embrace transparency and help their customers understand how their data is being used.

Methodology

The survey was commissioned by Okta, and carried out by Juniper Research. It was distributed and completed through an online platform.

The survey was carried out using an online panel in two waves, between the dates of 20th and 31st January 2020 and 27th April to 6th May. The survey was a nationally representative sample of the online population aged between 18 and 75 of each of the following countries, in the local language:

- Australia (2,002 respondents in wave 1, 947 in wave 2)
- France (2,000 respondents in wave 1, 973 in wave 2)
- Germany (2,000 respondents in wave 1, 936 in wave 2)
- The Netherlands (2,006 respondents in wave 1, 1,004 in wave 2)
- The United Kingdom (2,218 respondents in wave 1, 979 in wave 2)
- The United States (2,013 respondents in wave 1, 923 in wave 2)

Confidence intervals at the 95% confidence level for all countries are $\pm 2.2\%$ for wave 1, and $\pm 3.2\%$ in wave 2. All data was weighted in line with nationally representative proportions.