

70% of Australians don't feel in control of their data as companies hide behind meaningless privacy terms

February 27 2024, by Katharine Kemp

Perceptions of control over what businesses do with personal information

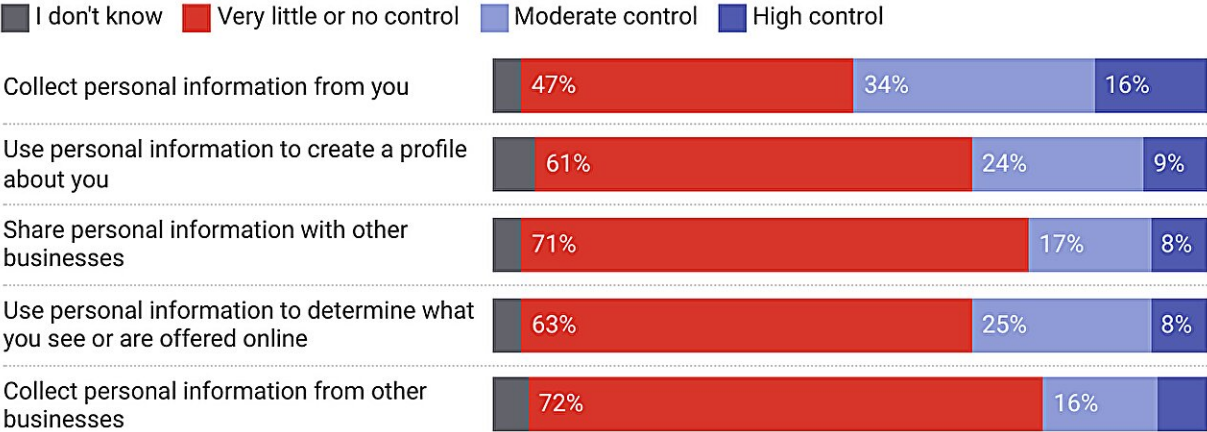


Chart: The Conversation • Source: Consumer Policy Research Centre, UNSW Sydney • Created with Datawrapper

Credit: The Conversation

Australian consumers don't understand how companies—including data brokers—track, target and profile them. This is revealed in new research on consumer understanding of privacy terms, released by the non-profit [Consumer Policy Research Centre](#) and UNSW Sydney today.

[Our report](#) also reveals 70% of Australians feel they have little or no control over how their data is disclosed between companies. Many expressed anger, frustration and distrust.

These findings are particularly important as the government considers [long-overdue reforms to our privacy legislation](#), and the [consumer watchdog](#) finalizes its [upcoming report on data brokers](#).

If Australians are to have any hope of fair and trustworthy data handling, the government must stop companies from [hiding their practices](#) behind confusing and misleading privacy terms and mandate fairness in data handling.

We are all being tracked

Our activities online and offline are constantly tracked by various companies, including [data brokers](#) that trade in our personal information.

This includes data about our activity and purchases on websites and apps, relationship status, children, financial circumstances, life events, [health concerns](#), search history and location.

Many businesses focus their efforts on finding new ways to track and profile us, despite repeated evidence that consumers view this as [misuse of their personal information](#).

Companies describe the data they collect in confusing and unfamiliar terms. Much of this wording seems designed to prevent us from understanding or objecting to the use and disclosure of our personal information, often collected in surreptitious ways.

Businesses can use your data [to make more profit at your expense](#). This includes

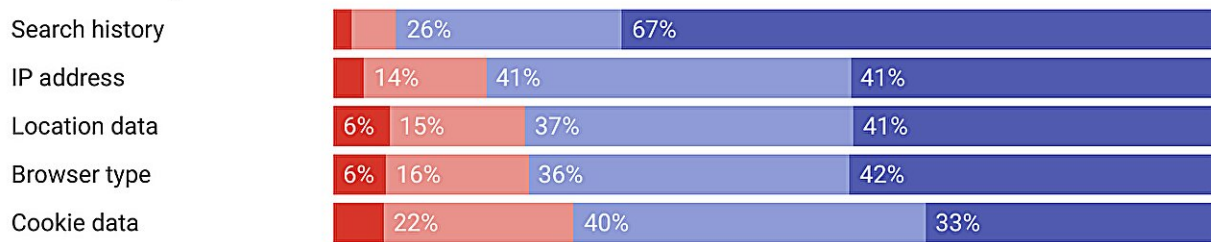
- charging you a higher price
- preventing you from seeing better offers
- micro-targeting [political messages](#) or ads based on your health information
- reducing the priority you're given in customer service
- creating a profile (which you'll never see) to share with a prospective employer, insurer or landlord.

Anonymized, pseudonymised, hashed

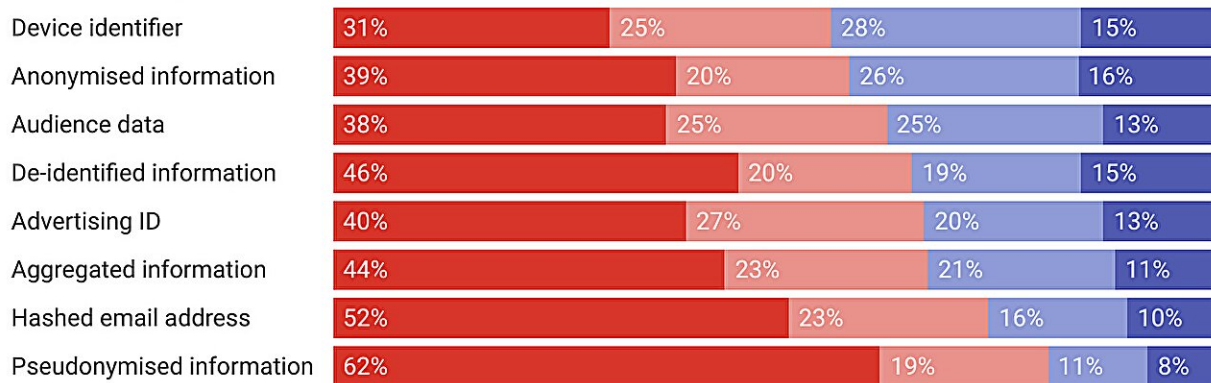
Familiarity with terms used in privacy policies

■ I've never seen this¹
■ I don't know this²
■ I know a bit³
■ I know a lot⁴

Most familiarity



Least familiarity



1: I've never seen this term / don't know what it is

2: I've seen it but know nothing about it

3: I know a little bit about this

4: I know a lot / quite a bit about this

Chart: The Conversation • Source: Consumer Policy Research Centre, UNSW Sydney • Created with Datawrapper

Credit: The Conversation

Businesses commonly try to argue this information is "[de-identified](#)" or not "[personal](#)", to avoid running afoul of the federal Privacy Act in which these terms are defined.

But many privacy policies muddy the waters by using other, undefined terms. They create the impression data can't be used to single out the consumer or influence what they're shown online—even when it can.

Privacy policies commonly refer to:

- anonymized data
- pseudonymised information
- hashed emails
- audience data
- aggregated information.

These terms have no legal definition and no fixed meaning in practice.

Data brokers and other companies may use "pseudonymised information" or "hashed email addresses" (essentially, encrypted addresses) to create detailed profiles. These will be shared with other businesses without our knowledge. They do this by matching the information collected about us by various companies in different parts of our lives.

"Anonymized information"—not a legal term in Australia—may sound like it wouldn't reveal anything about an individual consumer. Some companies use it when only a person's name and email have been removed, but we can still be identified by other unique or rare

characteristics.

What did our survey find?

Our survey showed Australians do not feel in control of their personal information. More than 70% of consumers believe they have very little or no control over what personal information online businesses share with other companies.

Only a third of consumers feel they have at least moderate control over whether businesses use their personal information to create a profile about them.

Most consumers have no understanding of common terms in privacy notices, such as "hashed email address" or "advertising ID" (a unique ID usually assigned to one's device).

And it's likely to be worse than these statistics suggest, since some consumers may overestimate their knowledge.

What personal info is acceptable for a business to use?

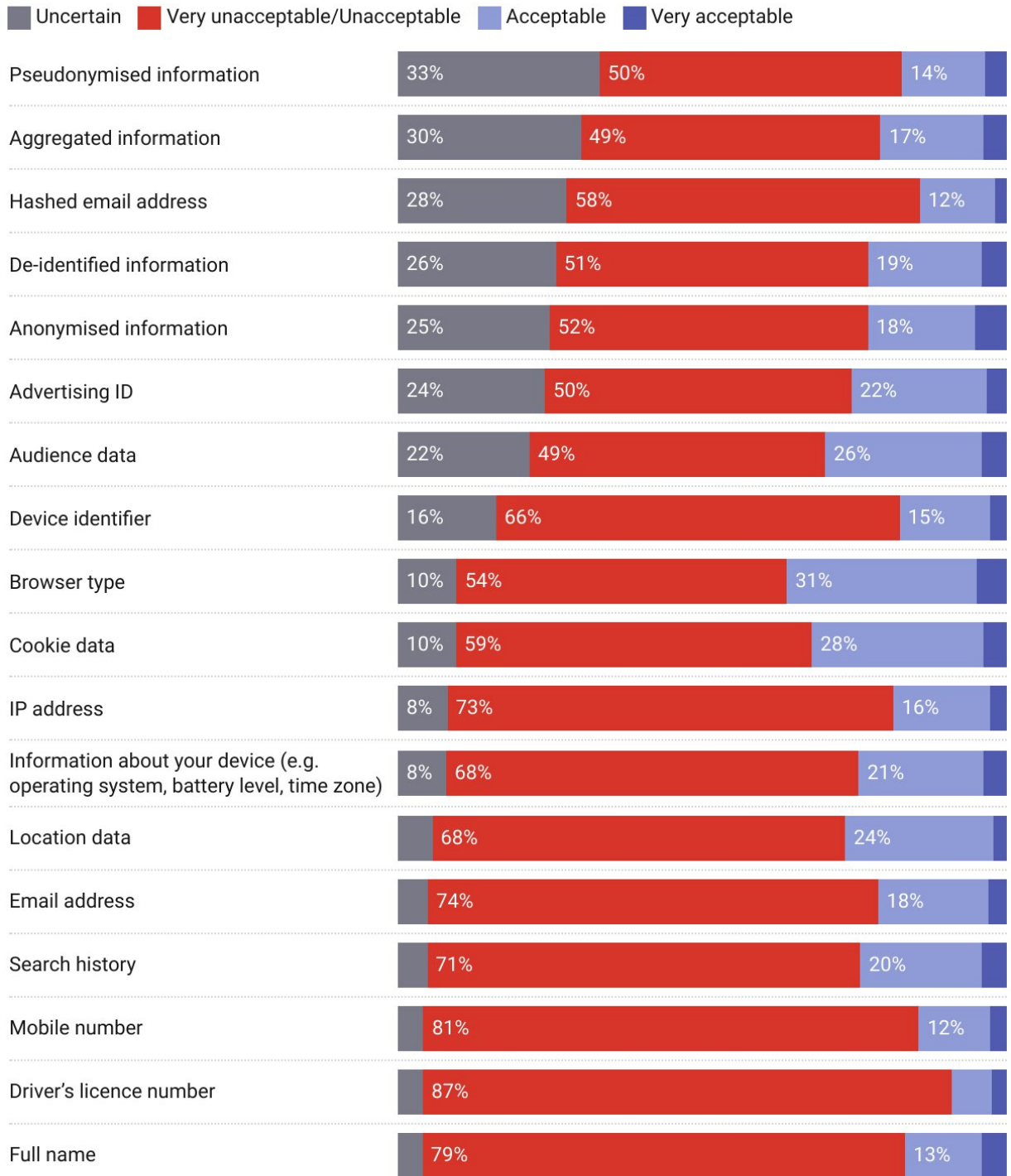


Chart: The Conversation • Source: Consumer Policy Research Centre, UNSW Sydney • Created with Datawrapper

Credit: The Conversation

The terms refer to data widely used to track and influence us without our knowledge. However, when consumers don't recognize descriptions of personal information, they're less likely to know whether that data could be used to single them out for tracking, influencing, profiling, discrimination, or exclusion.

Most consumers either don't know, or think it unlikely, that "pseudonymised information," a "hashed email address" or "advertising ID" can be used to single them out from the crowd. They can.

Most consumers think it's unacceptable for businesses they have no [direct relationship](#) with to use their email address, IP address, device information, search history or location data. However, data brokers and other "data partners" not in direct contact with consumers commonly use such data.

Consumers are understandably frustrated, anxious, and angry about the unfair and untrustworthy ways organizations make use of their personal information and expose them to increased risk of data misuse.

Fairness, not 'education'

Simply educating consumers about the terms used by companies and the ways their data is shared may seem an obvious solution.

However, we don't recommend this for three reasons. Firstly, we can't be sure of the meaning of undefined terms. Companies will likely keep coming up with new ones.

Secondly, it's unreasonable to place the burden of understanding complex data ecosystems on consumers who naturally lack expertise in

these areas.

Thirdly, "education" is pointless when consumers are not given real choices about the use of their data.

Urgent law reform is needed to make Australian privacy protections fit for the digital era. This should include clarifying that information that [singles an individual out from the crowd](#) is "personal information."

We also need a "fair and reasonable" test for data handling, instead of take-it-or-leave-it privacy "consents."

Most of us can't avoid participating in the digital economy. These changes would help ensure that instead of confusing privacy terms, there are substantial, meaningful legal requirements for how our [personal information](#) is handled.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: 70% of Australians don't feel in control of their data as companies hide behind meaningless privacy terms (2024, February 27) retrieved 27 April 2024 from <https://techxplore.com/news/2024-02-australians-dont-companies-meaningless-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.