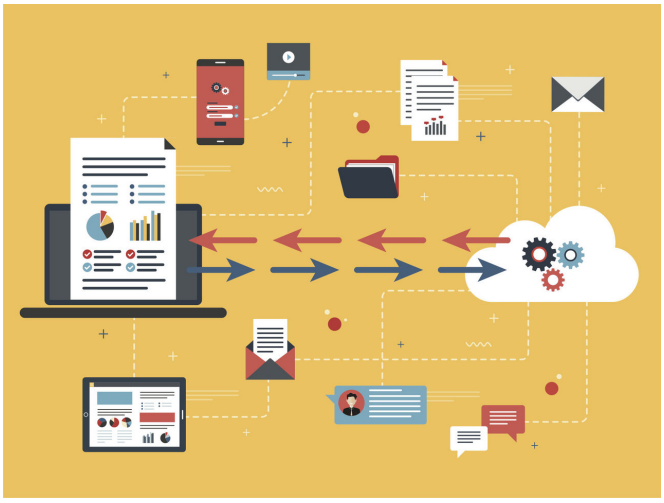
Soft terms like 'open' and 'sharing' don't tell the true story of your data

1 May 2018, by Katharine Kemp



Advances in machine learning may allow data that is de-identified now to be re-dentified in the future. Credit: www.shutterstock.com

The Turnbull government today announced the creation of a new National Data Commissioner to oversee the implementation of greater data access and "sharing" in Australia.

This follows the government's announcement late last year of a "consumer data right" relating to banking, energy, phone and internet transactions. This has been promoted as a means for Australians: "(…) to compare offers, get access to cheaper products and plans to help them "make the switch" and get greater value for money."

But we argue that the choice of words like "openness" and "sharing" hides the true nature of a rushed and risky proposal for our data.

It's time the government used more accurate language and less spin, so we can have a realistic debate about its plans *before* our personal information is irrevocably exposed.

'Open banking' within 12 months

For some years, the Australian government has pushed for increased data disclosure and linking in pursuit of efficiency and international competitiveness. It argues that access to more data will allow businesses to plan and adapt their offerings more efficiently, and that "big data" analytics will lead to increased innovation.

In 2017, the Productivity Commission backed this proposal – referring to the need for increased "openness" and "access". It recommended increased disclosure and use of data, including our personal and sensitive information.

The Commission does concede we, the public, might be wary of exposing our information. As a result, it has suggested that to gain necessary acceptance or "social licence", the government should create a new "consumer data right" allowing us to transfer our data to providers to get better offers.

The government is currently considering the Final Report of the Review into Open Banking, released in February. This recommends opening up data within 12 months for financial services, followed by other sectors.

In our opinion, this haste seems to be driven by FOMO (fear of missing out) – a sense that the world is talking big data and Australia shouldn't be left behind.

Inadequate privacy protection

What should be more troubling is that Australia already lags behind on the basic privacy protections that could make the planned data disclosure safe (or at least less risky).

Unlike most comparable countries advocating open data (including the US, UK and NZ), Australians

have no right to take anyone to court for a serious invasion of our privacy.

This is the case even though the Australian Law Reform Commission recommended this back in 2014 (after a near-identical recommendation in 2008) and the High Court called for action in 2001.

What's more, obligations under the Australian Privacy Act don't apply to the overwhelming majority of businesses – and experts criticise the weak enforcement of its already weak remedies.

In large part, the Privacy Act makes you responsible for protecting your privacy. Under the Australian law, if you continue to use a website after it has provided a link to its privacy policy, your consent is taken to be implied by that continued use. Consent does not even require ticking of a box in this context.

Where's the harm?

While few of us have celebrity-level secrets that might make us obsess over protection from paparazzi, the reality is in future we could suffer from weak privacy protections far more than any celebrity or politician.

If open banking goes ahead under current law, here's what's likely. When you agree to transfer your banking information from your existing bank to another provider via an Application Programming Interface (API), that provider will require you to tick a box saying you agree to its terms and conditions.

Those terms will include a privacy policy saying you consent to the new provider storing your data, giving it to others, and using it for other things, including vague "marketing purposes". Words in such policies typically state, for example: "(…) we may collect your personal information for research, marketing, for efficiency purposes (…)"

The new provider, and subsequent recipients, may combine that data with other personal information about you – collected from data aggregating giants like Acxiom, Facebook and Google – and use it to create a 360-degree, "God-like view" of you as an individual.

This can be used to create scores, psychographic profiles and predictions based on your spending, friends, health, race, sexual orientation, political affiliation, and lifestyle choices.

Such aggregated data could potentially be used to exploit, manipulate or discriminate against you based on your needs and weaknesses.

The Final Report of the Review into Open Banking accepted these plans would increase data security risks from hacking, improper disclosure and access. It recommended some improvements to consumer consent processes.

But it didn't recommend the essential change to substantive privacy law: to give us the right to sue, or increased penalties for breaches, or to give us a right to have our data deleted once it's been used for its original purpose.

The Productivity Commission proposed anonymisation or de-identification of your data to reduce risks. But advances in big data and machine learning for re-identification overtake attempts to de-identify, so data previously thought safe to release later becomes unsafe.

Attending a recent blockchain conference in Sydney, we heard a computer scientist say that, given a choice, he wouldn't agree to the release of his anonymised medical record because he's sure it will be re-identified – as his record – within the decade.

Not 'openness', not 'sharing'

It's misleading to talk of these data practices as "openness" and "sharing". These are just feel-good marketing terms to evoke positive emotions and hide reality.

The government's proposal does not make data more open. It encourages us to consent to vast exposure of our personal information, including to those who may use it against us, for example, through vulnerability-based marketing.

The UN's Special Rapporteur on Privacy has noted that open data originally referred to governments

making information about *government* and "the world we live in" more accessible to citizens; but it's now used to refer to governments and corporations releasing personal information about *citizens*.

It's also misleading to call this sharing. "Sharing" suggests a safe relationship with someone you know and trust; a friendly interaction which ends with you taking back your book or your bike or your holiday photos.

It does not reflect an irrevocable transfer of your personal information to an unknown corporation – which can keep it indefinitely, use it as they see fit, and give it to other countries and entities regardless of your interests.

Instead of talking about some undefined social licence for opening up data and sharing our personal information, the Australian government should start a more transparent discussion. It should use neutral words with practical meaning and known legal implications, like collection, use, storage, transfer and disclosure. The government should also highlight the risks of weak data protection.

This would be a real conversation about one stakeholder seeking to gain the trust of another, and what it would take for the trust-seeker to be viewed as trust-worthy.

This article was originally published on The Conversation. Read the original article.