Keep calm, but don’t just carry on: how to deal with China’s mass surveillance of thousands of Australians

September 14, 2020 4.50pm AEST

National security is like sausage-making. We might enjoy the tasty product, but want to look away from the manufacturing.

Recent news that Chinese company Zhenhua Data is profiling more than 35,000 Australians isn’t a surprise to people with an interest in privacy, security and social networks. We need to think critically about this, knowing we can do something to prevent it from happening again.

Reports indicate Zhenhua provides services to the Chinese government. It may also provide services to businesses in China and overseas.

The company operates under Chinese law and doesn’t appear to have a presence in Australia. That means we can’t shut it down or penalise it for a breach of our law. Also, Beijing is unlikely to respond
to expressions of outrage from Australia or condemnation by our government – especially amid recent sabre-rattling.

Read more: *Journalists have become diplomatic pawns in China’s relations with the West, setting a worrying precedent*

Zhenhua is reported to have data on more than 35,000 Australians – a list saturated by political leaders and prominent figures. Names, birthdays, addresses, marital status, photographs, political associations, relatives and social media account details are among the information extracted.

It seems Zhenhua has data on a wide range of Australians, including public figures such as Victorian supreme court judge Anthony Cavanough, Australia’s former ambassador to China Geoff Raby, former NSW premier and federal foreign affairs minister Bob Carr, tech billionaire Mike Cannon-Brookes and singer Natalie Imbruglia.

Former NSW premier Bob Carr is one of thousands of Australians who have had their information collected. Joel Carrett/AAP

It’s not clear how individuals are being targeted. The profiling might be systematic. It might instead be conducted on the basis of a specific industry, academic discipline, public prominence or perceived political influence.

It’s unlikely Zhenhua profiles random members of the public. That means there’s no reason for average citizens without a China connection to be worried.
Still, details around the intelligence gathering elude us, so best practise for the public is to maintain as much online privacy as possible, whenever possible.

Overall, we don’t know much about Zhenhua’s goals. And what we do know came from a leak to a US academic who sensibly fled China in 2018, fearing for his safety.

**Pervasive surveillance is the norm**

Pervasive surveillance is now a standard feature of all major governments, which often rely on surveillance-for-profit companies. Governments in the West buy services from big data analytic companies such as Palantir.

Australia’s government gathers information outside our borders, too. Take the bugging of the Timor-Leste government, a supposed friend rather than enemy.

**How sophisticated is the plot?**

Revelations about Zhenhua have referred to the use of artificial intelligence and the “mosaic” method of intelligence gathering. But this is probably less exciting than it sounds.

Reports indicate much of the data was extracted from online open sources. Access to much of this would have simply involved using algorithms to aggregate targets’ names, dates, qualifications and work history data found on publicly available sites.

The algorithms then help put the individual pieces of the “mosaic” together and fill in the holes on the basis of each individual’s relationship with others, such as their as peers, colleagues or partners.

Some of the data for the mosaic may come from hacking or be gathered directly by the profiler. According to the ABC, some data that landed in Zhenhua’s lap was taken from the dark web.

One seller might have spent years copying data from university networks. For example, last year the Australian National University acknowledged major personal data breaches had taken place, potentially extending back 19 years.

This year there was also the unauthorised (and avoidable) access by cybercriminals to NSW government data on 200,000 people.

While it may be confronting to know a foreign state is compiling information on Australian citizens, it should be comforting to learn sharing this information can be avoided – if you’re careful.

**What’s going on in the black box?**

One big question is what Zhenhua’s customers in China’s political and business spheres might do with the data they’ve compiled on Australian citizens. Frankly, we don’t know. National security is often a black box and we are unlikely ever to get verifiable details.
Apart from distaste at being profiled, we might say being watched is no big deal, especially given many of those on the list are already public figures. Simply having an AI-assisted “Who’s Who” of prominent Australians isn’t necessarily frightening.

However, it is of concern if the information collected is being used for disinformation, such as through any means intended to erode trust in political processes, or subvert elections.

For instance, a report published in June by the Australian Strategic Policy Institute detailed how Chinese-speaking people in Australia were being targeted by a “persistent, large-scale influence campaign linked to Chinese state actors”.

Deep fake videos are another form of subversion of increasing concern to governments and academics, particularly in the US.

**Read more:** Deepfake videos could destroy trust in society – here’s how to restore it

**Can we fix this?**

We can’t make Zhenhua and its competitors disappear. Governments think they are too useful.

Making everything visible to state surveillance is now the ambition of many law enforcement bodies and all intelligence agencies. It’s akin to Google and its competitors wanting to know (and sell) everything about us, without regard for privacy as a human right.

We can, however, build resilience.
One way is to require government agencies and businesses to safeguard their databases. That hasn’t been the case with the NSW government, Commonwealth governments, Facebook, dating services and major hospitals.

In Australia, we need to adopt recommendations by law reform inquiries and establish a national right to privacy. The associated privacy tort would incentivise data custodians and also encourage the public to avoid oversharing online.

In doing so, we might be better placed to condemn both China and other nations participating in unethical intelligence gathering, while properly acknowledging our own wrongdoings in Timor-Leste.