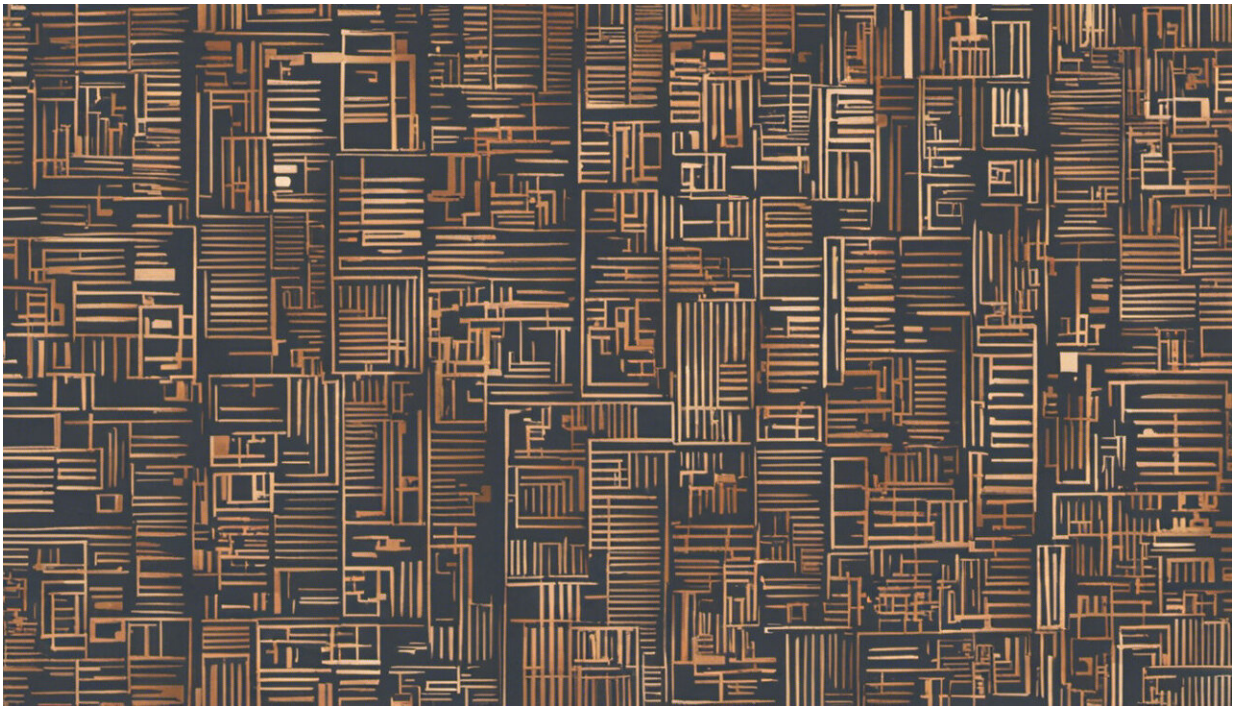
What do TikTok, Bunnings, eBay and Netflix have in common? They're all hyper-collectors

July 21 2022, by Brendan Walker-Munro



Credit: AI-generated image (disclaimer)

You walk into a shopping centre to buy some groceries. Without your knowledge, an electronic scan of your face is taken by in-store surveillance cameras and stored in an online database. Each time you return to that store, your "faceprint" is compared with those of people wanted for shoplifting or violence.

This might sound like science fiction but it's the reality for many of us. By failing to take our digital privacy seriously—as former human rights commissioner Ed Santow has warned—Australia is "sleepwalking" its way into mass surveillance.

Privacy and the digital environment

Of course, companies have been collecting personal information for decades. If you've ever signed up to a loyalty program like FlyBuys then you've performed what marketing agencies call a "value exchange". In return for benefits from the company (like discounted prices or special offers), you've handed over details of who you are, what you buy, and how often you buy it.

Consumer data is big business. In 2019, a report from digital marketers WebFX showed that data from around 1,400 loyalty programs was routinely being traded across the globe as part of an industry worth around US$200 billion. That same year, the Australian Competition and Consumer Commission's review of loyalty schemes revealed how many of these loyalty schemes lacked data transparency and even discriminated against vulnerable customers.

But the digital environment is making data collection even easier. When you watch Netflix, for example, the company knows what you watch, when you watch it, and how long you watch it for. But they go further, also capturing data on which scenes or episodes you watch repeatedly, the ratings of your content, the number of searches you perform and what you search for.

Hyper-collection: a new challenge to privacy

Late last year, the controversial tech company ClearView AI was

ordered by the Australian information commissioner to stop "scraping" social media for the pictures it was collecting in its massive facial recognition database. Just this month, the commissioner was investigating several retailers for creating facial profiles of the customers in their stores.

This new phenomenon—"hyper-collection"—represents a growing trend by large companies to collect, sort, analyse and use more information than they need, usually in covert or passive ways. In many cases, hyper-collection is not supported by a truly legitimate commercial or legal purpose.

Digital privacy laws and hyper-collection

Hyper-collection is a major problem in Australia for three reasons.

First, Australia's privacy law wasn't prepared for the likes of Netflix and TikTok. Despite numerous amendments, the Privacy Act dates back to the late 1980s. Although former Attorney-General Christian Porter announced a review of the Act in late 2019, it has been held up by the recent change of government.

Second, Australian privacy laws are unlikely on their own to threaten the profit base of foreign companies, especially those located in China. The Information Commissioner has the power to order companies to take certain actions—like it did with Uber in 2021—and can enforce these through court orders. But the penalties aren't really big enough to discourage companies with profits in the billions of dollars.

Third, hyper-collection is often enabled by the vague consents we give to get access to the services these companies provide. Bunnings, for example, argued that its collection of your faceprint was allowed because signs at the entry to their stores told customers facial recognition might

be used. Online marketplaces like eBay, Amazon, Kogan and Catch, meanwhile, supply "bundled consents"—basically, you have to consent to their privacy policies as a condition of using their services. No consent, no access.

TikTok and hyper-collection

TikTok (owned by Chinese company ByteDance) has largely replaced YouTube as a way of creating and sharing online videos. The app is powered by an algorithm has already drawn criticism for routinely collecting data about users, as well as the ByteDance's secretive approach to content moderation and censorship.

For years, TikTok executives have been telling governments that data isn't stored in servers on the Chinese mainland. But these promises might be hollow in the wake of recent allegations.

Cybersecurity experts now claim that not only does the TikTok app routinely connect to Chinese servers, but that users' data is accessible by ByteDance employees, including the mysterious Beijing-based "Master Admin", which has access to every user's personal information.

Then, just this week, it was alleged that TikTok (owned by Chinese company ByteDance) can also access almost all the data contained on the phone it is installed on—including photos, calendars and emails.

Under China's national security laws, the government can order tech companies to pass on that information to police or intelligence agencies.

What options do we have?

Unlike a physical store, we don't get a lot of choice about consenting to

digital companies' privacy policies and how they collect our information.

One option—supported by encryption expert Vanessa Teague at ANU—is for consumers simply to delete offending apps until their creators are willing to submit to greater data transparency. Of course, this means locking ourselves out of those services, and it will only have a big impact in the company if enough Australians join in.

Another option is "opting-out" of intrusive data collection. We've done this before—when My Health records became mandatory in 2019, a record number of us opted out. Though these opt-outs reduced the usefulness of that digital health record program, they did demonstrate that Australians can take their data privacy seriously.

But how exactly can Australians opt-out of a massive social app like TikTok? Right now, they can't—perhaps the government needs to explore a solution as part of its review.

A further option being explored by the Privacy Act review is whether to create new laws that would allow individuals to sue companies for damages for breaches of privacy. While lawsuits are expensive and time-consuming, they might just deliver the kind of financial damage to big companies that could change their behaviour.

No matter which option we take, Australians need to start getting more savvy with their data privacy. This might just mean we actually read those terms and conditions before agreeing, and being prepared to "vote with our feet" if companies won't be honest about what they're doing with our personal information.

Provided by The Conversation