When Big Brother gets too smart . . . worry

Juha Saarinen comment

If you have a spare three-quarters of an hour, listen to last Sunday's episode on National Radio's Raising the Bar programme featuring engineer and University of Auckland researcher Andrew Chen.

It was recorded last year with Chen wanting to draw our attention to the myriad of CCTV cameras that are popping up everywhere and how they are being repurposed for what is essentially surveillance tools.

He's concerned about the consequences of using these as silent, unobtrusive data collection tools that monitor our moves in public spaces, supermarkets, services stations – everywhere really.

Depending on how they're used, and by whom, the data collection can be good or bad for us when it's coupled with myriads of other information sources.

As an example, Chen mentioned that Japanese tech giant NEC worked with the councils in Wellington and Christchurch using CCTV cameras to measure pedestrian movements and volumes between 2014 and this year.

That sounds useful but Chen told me "mission creep" set in, and NEC wanted to sell the data to retailers and tourism operators.

Ironically, while it's apparently fine to record people in public via CCTV cameras, intercepting conversations isn't so the audio capture had to be turned off as it was illegal.

Auckland was interested too but was concerned about the privacy impact and didn't end up using analytics with the city's CCTV camera systems, Chen said.

He said the trial was shut late last year, probably for commercial rather than privacy reasons.

It shows how easy it is to tip the balance away from something that's useful for people towards unknown third parties as data collected by retailers is onsold, say to insurance companies. One example would be a health insurer wanting to monitor customers. A fast-food outlet might be selling data from customer visits and orders to a marketing analytics company, but what if that information also goes elsewhere?

Yes, there are ways to de-identify sensitive data to make the use of it less privacy invasive. Most such data can be re-identified partly or fully as researchers have shown.

To reduce its liabilities, an insurer might deem there are commercial incentives to obtain customer visit data from the analytics firm.

The data could be correlated with other sources of information, including locations from smartphones and facial recognition from networked cameras, to provide a reasonably accurate summary of individuals' fast-food habits.

This shows the importance of having control over the data that's being recorded. Once it shifts from one context to another, one that uses information gathered in a completely different way to the original, the consequences can be severe.

Despite the additional revenue onselling customer visit data brings in for fast-food chains, my bet is they would not want people to stop going out for burgers and fries because their eating habits are being leaked to insurers, leading to premium hikes or policy cancellations.

This is big-picture stuff that requires thought, discussion and regulation because the technology that watches and analyses what we do isn't going away.

Chen suggests there should be limits placed on data collection gear so the information stays on the devices and is processed for a specific purpose within a specific time after which it is deleted.

This would protect our privacy, but is costlier to implement in devices. Also, data collectors couldn't resell the information to third parties which is a commercial disincentive.

Given how easy it is to keep a tireless eye on people with technology, we need to place some sensible regulatory limits on data collected via automated surveillance. Shifting it from the public good context to a strictly commercial one risks producing hair-raisingly bad outcomes for everyone.

Photo / Getty Images