The Sydney Morning Herald

Technology Information security

This was published 3 years ago

If you go down to the mall today, you're watched by a thousand eyes

By **Garreth Hanley**

December 15, 2017 — 1.57pm

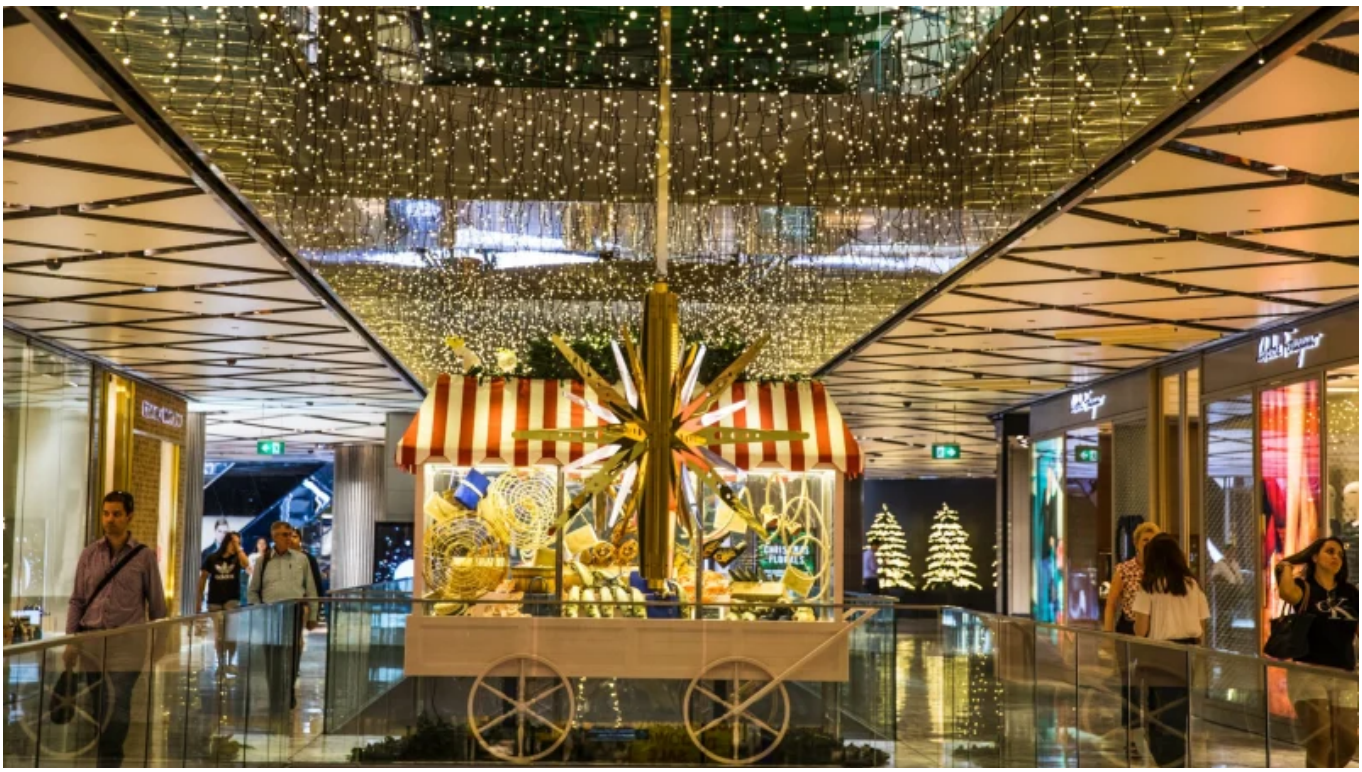
You need a new pair of shoes.

En route to the shopping centre, you pull into a service station. Filling up the fuel tank, you distractedly watch ads on a small screen on the bowser.

Illustration: Richard Giliberto

Meanwhile, the intelligence system at work behind the screen gets a fix on your age and gender. Are you wearing spectacles, or a beard? Having classified you into one of 18 demographic profiles, it serves up a targeted ad, and monitors your mood as the ad is being played. This information is then relayed back to advertisers so they can fine-tune their pitch.

The purveyors of this "Digital-outdoor Audience in Real Time" analysis – or DART – boast that it is "anonymously tracking over 2 million Australians weekly".



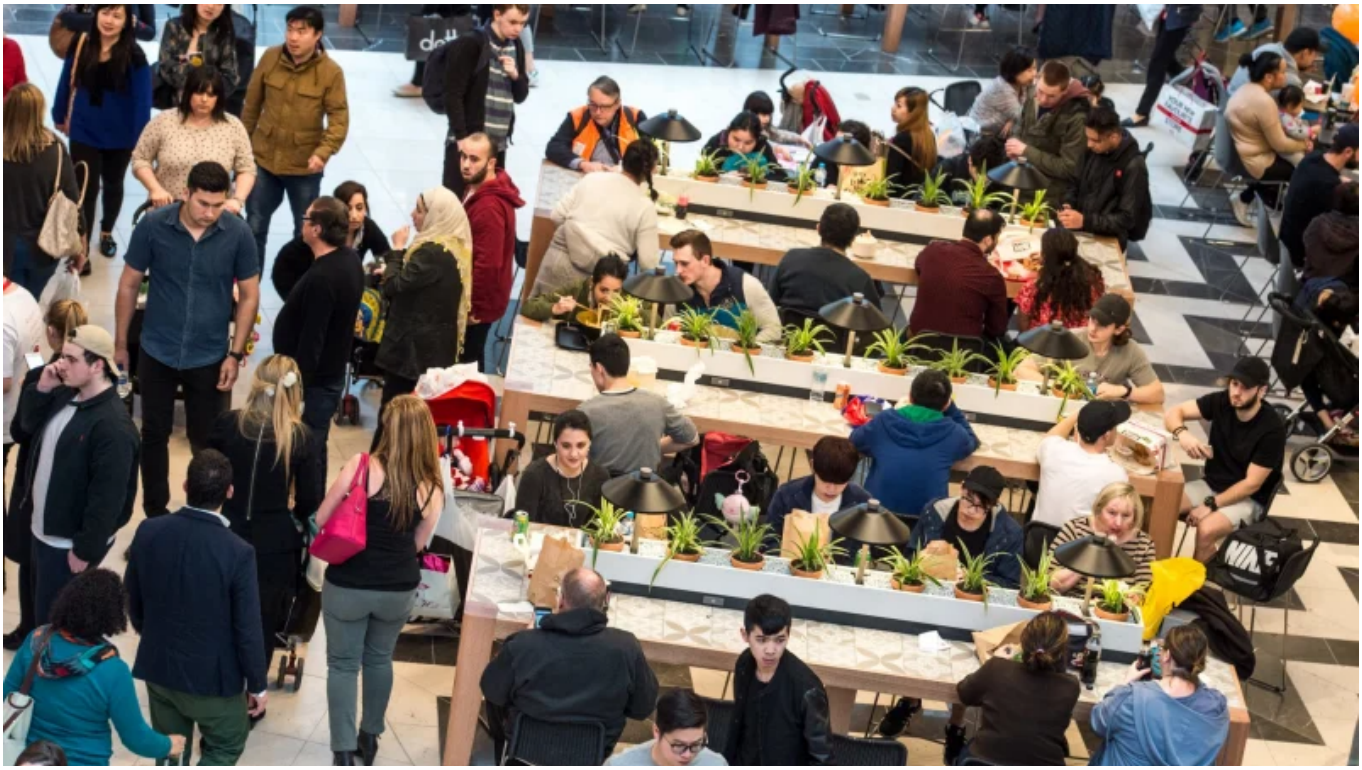
Westfield collects movement data about everyone who visits its centres. JESSICA HROMAS

Arriving at the shopping centre car park, your number plate is scanned. You walk into the mall, passing a discreet sign: "To improve your experience, we provide free WiFi and use WiFi monitoring in this centre. Please adjust your device settings to opt out of this service."

The phone in your pocket leaves a trail of data breadcrumbs: where you linger, where you hurry on.

You pause in front of an advertising screen. Again, it's watching you, rapidly curating the flow of advertising to match your demographic profile. You go to the shoe store and select a pair. Along with your credit card, you hand over a loyalty card in return for a modest bonus some time down the track.

You've got your new shoes, and in the process delivered a trove of information which is swapped and shared between retailing networks. Even as your time of exit from the car park is uploaded, corporations are fine-tuning their next hit on your hip pocket.

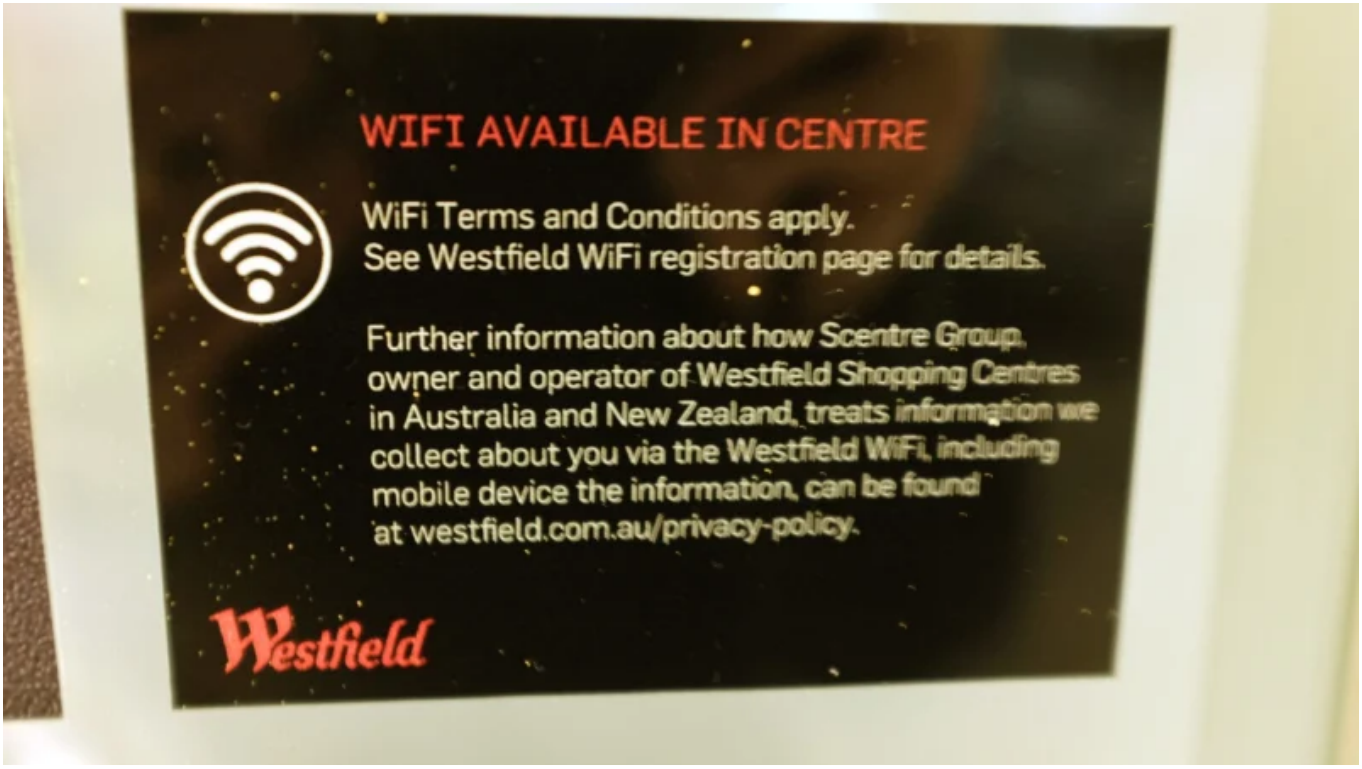


Chadstone Shopping Centre is part of Vicinity's portfolio. PENNY STEPHENS

From security to selling

Sophisticated facial recognition and video surveillance systems routinely used to secure airports and other high-security zones are now also being turned on to consumers by retailers – and not just to track and catch shoplifters.

These developments are part of a rapidly expanding array of systems keeping close tabs on Australian shoppers, monitoring purchasing habits, tracking mobile phone locations, accessing web browsing history, identifying an individual shopper's demographic profile, and even using emotion recognition software to read mood.



A sign advertising free WiFi outside a Westfield shopping centre. GARRETH HANLEY

In a recent BBC forum on the commercial use of biometric data, a former head of the UK Border Force, Tony Smith, warned that governments need to legislate to head off the inappropriate use of new surveillance technologies.

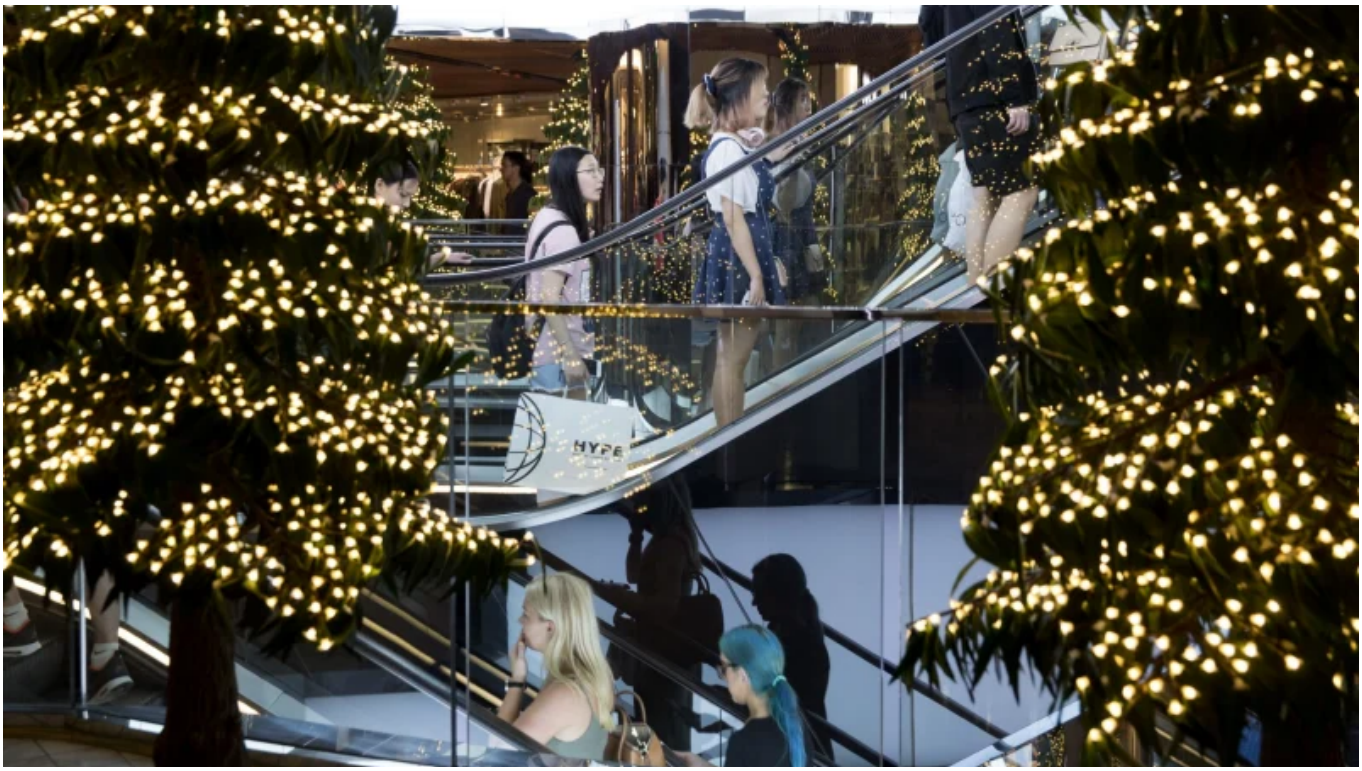
Questioned about his concerns, Smith said: "Private-sector entities like stores having their own database of photographs" was an unexpected development.

The DFO at South Wharf.

"It started as security, but is now being used for marketing," he added, and "legislation needs to put down gateways where the data is being used inappropriately, and currently it isn't doing

that."

Australian experts are also sounding the alarm. "The law and regulatory frameworks have lagged behind technological developments and this presents serious privacy and also information security concerns," says Dr Monique Mann, a specialist in privacy law at the Queensland University of Technology.



We're entering a reality of "uberveillance", says Dr Katina Michael. JANIE BARRETT

The global retail biometric market is set to reach $1.6 billion in 2020, up from $625 million in 2015, according to the 2017 Deloitte Consumer Review.

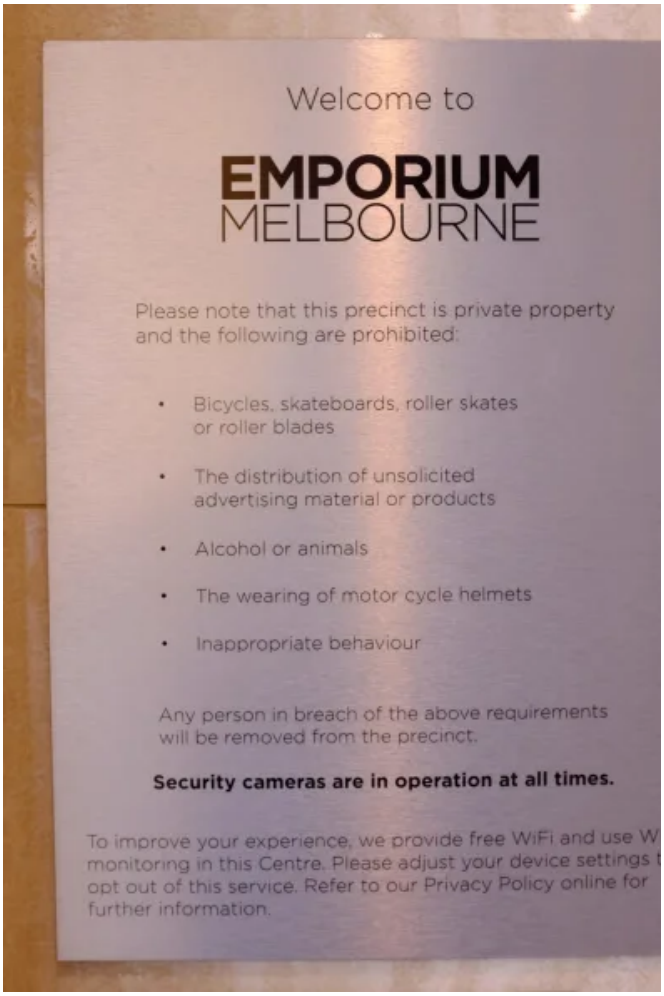
In Australia, major shopping centre chains Scentre Group, which runs Westfield Centres, and Vicinity Centres, which includes DFO and Chadstone Shopping Centre in Melbourne and Chatswood Chase in Sydney, collect movement data about everyone who visits their centres. Meanwhile, advertising giant Val Morgan is rolling out facial recognition and mood analysis advertising screens that serve customised ads after scanning the face of whoever is looking at the screen.

The only clue shoppers have to the armoury of devices and systems tracking them is in the fine print on the small signs they pass as they enter centres. Typically, these signs outline terms of entry and alert people to the possibility of data collection, but usually they direct people to a "privacy policy" webpage for more details. The very act of entering the shopping centre implies you have read and agreed to these terms.

Some of the signs clearly state your mobile phone will be tracked unless you "change the settings on your device", but they provide no instructions about what settings need to be changed, or how they are tracking you.

Vicinity's privacy policy webpage states it may collect, among other things, your name, date of birth, address and other contact details, details of your interests and shopping preferences and activity, information about your visits to its shopping centres collected through the WiFi or mobile application, including "device identifiers, usage and location data".

Westfield also collects personal information and its privacy policy states the centre tracks customers' mobile phones. It says: "Where devices are enabled to connect to, or are identifiable by, in-centre infrastructure (for example, in-centre WiFi networks or bluetooth transmitter [beacon] infrastructure), we and our third party providers may automatically collect data from those devices including usage, type of device and location and proximity of your wireless device in-Centre, centre arrival and departure time."



The sign outside Emporium Melbourne. GARRETH HANLEY

These systems are being combined with sophisticated analytics in such granular detail that they can see how long a single customer might linger in front of a display, even "what shelves you are looking at and for how long", explains Dr Katina Michael, an information technology and law expert at the University of Wollongong.

The technology is also being deployed outside shopping centres, with Val Morgan rolling out its DART 2.0 intelligent screens at service stations nationwide. The company claims the information it collects and sells is anonymous.

But experts say that there is little comfort in this for consumers. Given that the data captured includes your gender, age, demographic markers, location and the time of your visit, it's no great leap to then figure out your identity, explains University of Melbourne expert in technology and cryptography Dr Vanessa Teague.

"Scientists have re-identified 'de-identified' data from mobility traces, health data, search queries, movie ratings, etc," Teague says. "As companies and criminals learn more information about people, re-identification only becomes easier.

"It's been shown over and over again, in a wide variety of different domains, that de-identification of complex individual records doesn't work."

Mann says that existing opt-in and opt-out programs, where a shopper might agree to data sharing when joining a rewards program, are quickly becoming an "outmoded concept of consent" and questions whether it is even possible to opt out in our increasingly connected society.

The information it scoops up can be super-enriched when combined with other sources of data, like the archive of detailed information shoppers with loyalty cards hand over to retailers at the cash register, or when it is linked to social media and internet usage data.

There is little regulatory capacity to enforce even existing rules, and very few protections for Australian consumers, says Dr Roger Clarke, an IT expert at the Australian National University

and a privacy advocate. The regulator, the Office of the Australian Information Commissioner (OAIC), is weak, he says. According to its last annual report, privacy complaints take an average of 4.7 months to complete.

Then there are the ethical and privacy questions posed by the creeping intrusion of surveillance. Earlier this month, Westpac Bank revealed it was trialling artificial intelligence-powered video cameras to read the mood of staff, "so leadership can take the pulse of their teams across the organisation".

We're entering a reality of "uberveillance", says Michael. She defines the term – which she coined with a colleague in a 2009 academic paper, and which has since made it into the Macquarie Dictionary – as "always-on, technology-enabled, pervasive surveillance systems integrated into society, electronic devices, and even the human body".

These systems are designed to monitor and monetise people, she says, by tracking their "identity, location and condition – knowing what someone is thinking, why they do what they do, and how they feel when they do it". These technologies reach into individuals in a new way, creating a profile that is best described as "behavioural biometrics", Michael says.

Consumer analysis per se is not new – many companies already collect detailed information about the members of their rewards programs. These opt-in programs all have the same aim, improving the bottom line of retailers and service providers, and some customers might be happy to trade off some privacy in return for emails with sales offers based on their previous purchases.

But that is not all the data can be used for. Loyalty programs also trade information about customer spending habits and lifestyles. It's in the fine print of the deal members agree to when they sign on.

For example, when a shopper swipes a Woolworths Rewards card at the supermarket checkout, the information on what is in his or her trolley is shared with a range of affiliated partners and any data can be combined with publicly available information and digital services used by the members – "including social media platforms". The card policy states this clearly: "At times, we combine different sets of data to add to the personal information we hold. An example of this is a history of a Member's transactions from use of the same payment card."

Both Westfield and Vicinity centres state they comply with the Australian Privacy Principles, and that the data they collect about visitors is used for "management and security purposes", and list the types of data they "may" collect when people enter their centres. However, they provide little information on what data they do collect, how they collect it, how it is stored, or what they use it for. Both companies also state they will share the data with their partners, and sometimes the information may be sent overseas.

I contacted management from both organisations for comment on their use of customer analytics, facial recognition technology and data collection.

Vicinity Centres declined to comment. However, in a statement to shareholders in August, Vicinity chief executive officer Angus McNaughton said: "Our consumers now have access to free high-speed WiFi at our centres and the rich data we are gathering from this network is enabling us to gain insight into consumer behaviour, including dwell times, foot traffic and the way foot traffic flows around our centres."

Scentre Group (Westfield) provided details about the marketing benefits of the data it collects, but did not respond when asked how it collects this information.

A version of this report was co-published in *The Citizen*, a publication of the University of Melbourne's Centre for Advancing Journalism.