Not Big Brother, but close: A surveillance expert explains some of the ways we're all being watched, all the time

December 19 2022, by Ausma Bernot

Credit: AI-generated image (disclaimer)

A group of researchers studied 15 months of human mobility movement data taken from 1.5 million people and concluded that just four points in space and time were sufficient to identify 95% of them, even when the data weren't of excellent quality.

That was back in 2013.

Nearly ten years on, surveillance technologies permeate all aspects of our lives. They collect swathes of data from us in various forms, and often without us knowing.

I'm a surveillance researcher with a focus on technology governance. Here's my round-up of widespread surveillance systems I think everyone should know about.

CCTV and open-access cameras

Although China has more than 50% of all surveillance cameras installed in the world (about 34 cameras per 1,000 people), Australian cities are catching up. In 2021, Sydney had 4.67 cameras per 1,000 people and Melbourne had 2.13.

While CCTV cameras can be used for legitimate purposes, such as promoting safety in cities and assisting police with criminal investigations, their use also poses serious concerns.

In 2021, New South Wales police were suspected of having used CCTV footage paired with facial recognition to find people attending anti-lockdown protests. When questioned, they didn't confirm or deny if they had (or if they would in the future).

In August 2022, the United Nations confirmed CCTV is being used to carry out "serious human rights violations" against Uyghur and other predominantly Muslim ethnic minorities in the Xinjiang region of Northwest China.

The CCTV cameras in China don't just record real-time footage. Many are equipped with facial recognition to keep tabs on the movements of

minorities. And some have reportedly been trialed to detect emotions.

The US also has a long history of using CCTV cameras to support racist policing practices. In 2021, Amnesty International reported areas with a higher proportion of non-white residents had more CCTV cameras.

Another issue with CCTV is security. Many of these cameras are open-access, which means they don't have password protection and can often be easily accessed online. So I could spend all day watching a livestream of someone's porch, as long as there was an open camera nearby.

Surveillance artist Dries Depoorter's recent project The Follower aptly showcases the vulnerabilities of open cameras. By coupling open camera footage with AI and Instagram photos, Depoorter was able to match people's photos with the footage of where and when they were taken.

There was pushback, with one of the identified people saying: "It's a crime to use the image of a person without permission."

Whether or not it is illegal will depend on the specific circumstances and where you live. Either way, the issue here is that Depoorter was able to do this in the first place.

IoT devices

An IoT ("Internet of Things") device is any device that connects to a wireless network to function— so think smart home devices such as Amazon Echo or Google Dot, a baby monitor, or even smart traffic lights.

It's estimated global spending on IoT devices will have reached US$1.2 trillion by some point this year. Around 18 billion connected devices form the IoT network. Like unsecured CCTV cameras, IoT devices are

easy to hack into if they use default passwords or passwords that have been leaked.

In some examples, hackers have hijacked baby monitor cameras to stalk breastfeeding mums, threaten parents that their baby was being kidnapped, and say creepy things like "I love you" to children.

Beyond hacking, businesses can also use data collected through IoT devices to further target customers with products and services.

Privacy experts raised the alarm in September over Amazon's merger agreement with robot vacuum company iRobot. A letter to the US Federal Trade Commission signed by 26 civil rights and privacy advocacy groups said, "Linking iRobot devices to the already intrusive Amazon home system incentivizes more data collection from more connected home devices, potentially including private details about our habits and our health that would endanger human rights and safety."

IoT-collected data can also change hands with third parties through data partnerships (which are very common), and this too without customers' explicit consent.

Big tech and big data

In 2017, the value of big data exceeded that of oil. Private companies have driven the majority of that growth.

For tech platforms, the expansive collection of users' personal information is business as usual, literally, because more data mean more precise analytics, more effective targeted ads and more revenue.

This logic of profit-making through targeted advertising has been dubbed "surveillance capitalism." As the old saying goes, if you're not

paying for it, then you're the product.

Meta (which owns both Facebook and Instagram) generated almost US$23 billion in advertising revenue in the third quarter of this year.

The vast machinery behind this is illustrated well in the 2021 documentary The Social Dilemma, even if in a dramatized way. It showed us how social media platforms rely on our psychological weaknesses to keep us online for as long as possible, measuring our actions down to the seconds we spend hovering over an ad.

Loyalty programs

Although many people don't realize it, loyalty programs are one of the biggest personal data collection gimmicks out there.

In a particularly intrusive example, in 2012 one US retailer sent a teenage girl a catalog dotted with pictures of smiling infants and nursery furniture. The girl's angered father went to confront managers at the local store, and learned that predictive analytics knew more about his daughter than he did.

It's estimated 88% of Australian consumers over age 16 are members of a loyalty program. These schemes build your consumer profile to sell you more stuff. Some might even charge you sneaky fees and lure you in with future perks to sell you at steep prices.

As technology journalist Ros Page notes:

"[T]he data you hand over at the checkout can be shared and sold to businesses you've never dealt with."

As a cheeky sidestep, you could find a buddy to swap your loyalty cards

with. Predictive analytics is only strong when it can recognize behavioral patterns. When the patterns are disrupted, the data turn into noise.

Provided by The Conversation