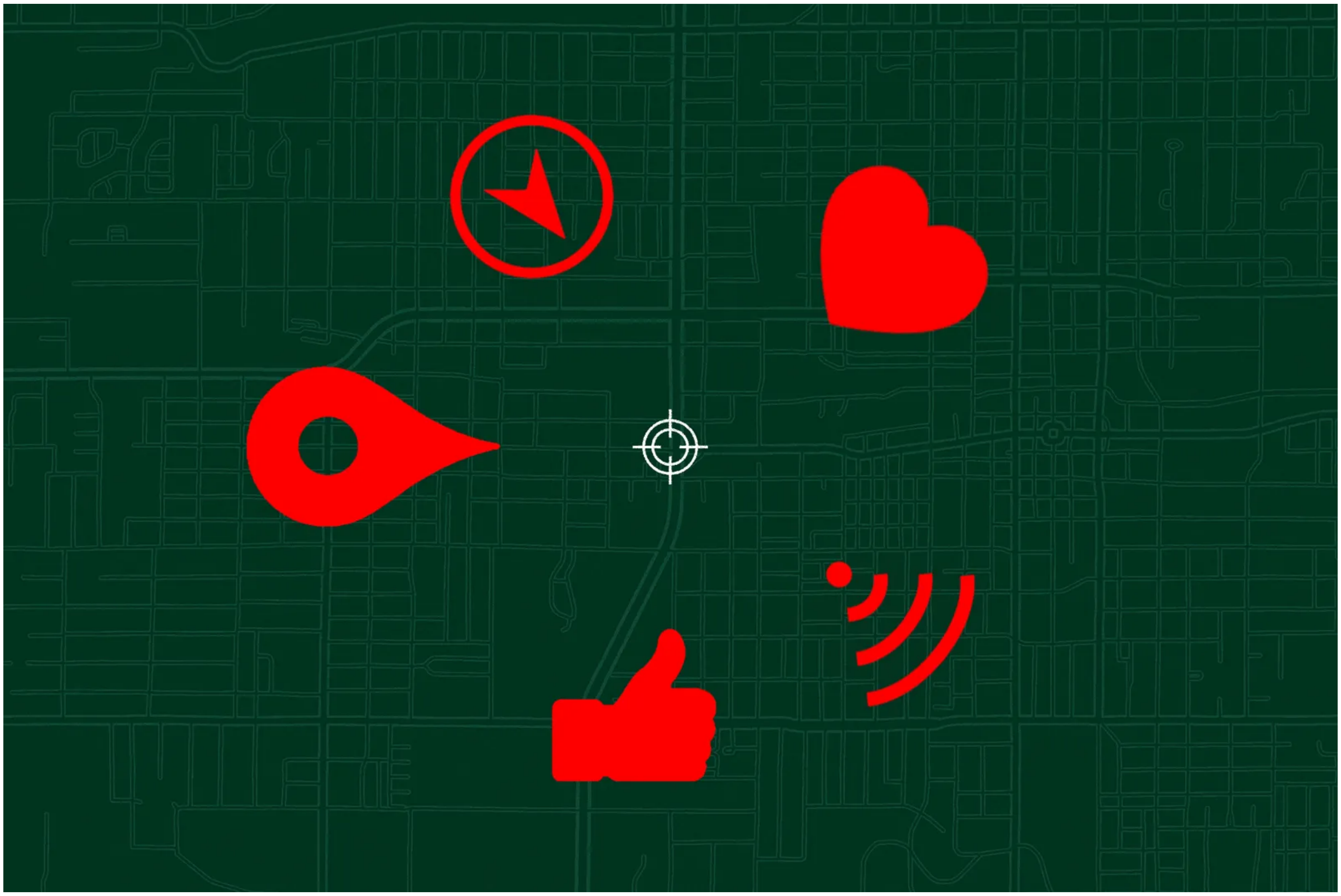
ELISE THOMAS CULTURE 16.09.2019 06:00 AM

New surveillance tech means you'll never be anonymous again

Forget facial recognition. Researchers around the world are creating new ways to monitor you. Lasers detecting your heartbeat and microbiome are already being developed



WIRED

The fight over the future of facial recognition is heating up. But it is just the beginning, as even more intrusive methods of surveillance are being developed in research labs around the world.

In the US, San Francisco, Somerville and Oakland recently banned the use of facial recognition by law enforcement and government agencies, while Portland is talking about forbidding the use of facial recognition entirely, including by private businesses. A coalition of 30 civil society organisations, representing over 15 million members combined, is calling for a federal ban on the use of facial recognition by US law enforcement.

Meanwhile in the UK, revelations that London's Metropolitan Police secretly provided facial recognition data to the developers of the Kings Cross Estate for a covert facial recognition system have sparked outrage and calls for an inquiry. The Information Commissioner's Office has launched an investigation into the legality of the program. But the scandal comes at the same time as a landmark ruling by the High Court in Cardiff that said the use of facial recognition by South Wales police is legal. (The decision is likely to be appealed).

Facial recognition is only the tip of the creepy surveillance iceberg, however. If strict regulation is brought in to govern the use of facial recognition, it is possible we may simply see a switch to one, or several, of the other forms of surveillance technologies currently being developed. Many are equally if not more invasive than facial recognition – and potentially even harder to regulate. Here's a look at some of what might be coming down the pipeline.

How you walk

The rapidly growing field of behavioural biometrics is based on recognising individuals from their patterns of movement or behaviour. One example is gait recognition, which may well be the next surveillance technology to hit the mainstream, especially if facial recognition comes under tight regulation. The technique is already being trialled by police in China, which frequently leads the field when it comes to finding new ways to monitor its people, whether they like it or not.

There are a few different ways of recognising an individual from the way they walk. The method being trialled by Chinese police is based on technology from a company called Watrix, and relies on the use of video surveillance footage to analyse a person's movements as they walk. In a recently granted patent, Watrix outlines a method of using a deep convolutional neural network to train an AI system capable of analysing thousands of data points about a person as they move, from the length of their stride to the angle of their arms, and use that to recognise individuals based on their 'gait record'. Watrix claims that its systems achieve up to 94 per cent accuracy, and that it holds the world's largest database of gait records.

The vision-based methods of gait recognition being developed by Watrix and others can be used to identify people at a distance, including in crowds or on the street, in a similar way that facial recognition can – which could make it a quick and easy substitute if regulation is brought in against facial recognition. Increasingly, many video surveillance systems are collecting multi-modal biometrics. That means they may be using facial recognition and gait recognition simultaneously, which at least in theory should both increase the accuracy and tackle issues like identifying people facing away from the cameras.

Another method for identifying people by their walk relies on sensors embedded in the floor. Researchers from the University of Manchester used data from 20,000 footsteps belonging to 127 individuals to train a deep residual neural network to recognise 24 distinct factors, like the person's stride cadence and the ratio of time on toe to time on heel (the people did not need to take off their shoes, as the system analyses movement rather than shape of the foot). Using this system, they were able to identify individuals with over 99 per cent accuracy in three 'real world' scenarios: the workplace, the home environment, and airport security checkpoints.

According to the researchers, the benefits of this kind of identification over vision-based systems are that it is less invasive, and less prone to disruption from objects or other people obscuring the camera's view. Of course, another way of saying that it is less invasive is that it is harder for people to detect when it's being used on them. People might notice when they're being watched by cameras, but they're much less likely to be aware of sensors in the floor.

Heartbeat detection

Your heartbeat and your breathing pattern are as unique as your fingerprint. A small but growing number of remote sensing technologies are being developed to detect vital signs from a distance, piercing through skin, clothes and in some cases even through walls.

In June, the Pentagon went public with a new laser-based system capable of identifying people at a distance of up to 200m. The technology, dubbed Jetson, uses a technique known as laser doppler vibrometry to detect surface movement caused by your heartbeat.

The eventual goal is to be able to identify a target within five seconds based on their cardiac signal, or 'heartprint.' At the moment, however, the Pentagon's system has a number of limitations: the target needs to be standing still, needs to be wearing light clothing (thick clothing, like a heavy coat, can interfere with the signal), and most importantly there needs to be a clear line of sight between the laser and the target.

Coats, walls, even rocks and rubble are no obstacle for another nascent surveillance technology, however. Researchers are hard at work developing radar-based systems capable of tracking vital signs for a range of purposes, from non-invasive monitoring of patients and aiding in medical diagnoses to finding survivors in search and rescue operations.

Monitoring indoor movements

But why bother installing new radars when we're already bathed in a different sort of radiation pretty much all the time? Wi-Fi can also be used to locate individuals, identify their position in the room and whether they're sitting or standing, and even track vital signs.

Until recently, it was thought a dedicated Wi-Fi network was required, in part because the technique depends on knowing the exact position of the Wi-Fi transmitters. In 2018, however, a group of researchers at the University of California built an app which allowed them to figure out the exact location of existing Wi-Fi transmitters in a building. With that information, they were able to use normal smartphones and existing ambient Wi-Fi networks to detect human presence and movement from outside the room. "With more than two Wi-Fi devices in a regular room, our attack can detect more than 99 per cent of user presence and movement in each room tested," the researchers claim.

Some research groups want to go further than just using Wi-Fi to identify people. Based on movement and vital signs, they claim it is possible to monitor the subject's emotional state and analyse their behavioural patterns. These researchers have formed a company to market a 'touchless sensor and machine learning platform for health analytics', which they claim has been deployed in over 200 homes and is being used by doctors and drug companies.

Beyond the potential benefits for healthcare and emergency responders, however, the technology also has obvious applications for surveillance. Technology which is capable of building up a profile of a person's heartbeat and breathing in order to watch for abnormalities in a health context is readily adaptable to being used to identify one person from another. Radar-based security surveillance systems capable of detecting people are already on the market, It's only a matter of time, and perhaps not even very much time, before the ability to identify individual people is layered on top.

Tracking your microbial cells

Every person emits around 36 million microbial cells per hour, and human microbiomes are unique for a certain period of time (a 2015 study found that around 80 per cent of people could be re-identified using their microbiome up to a year later). This means that the constant trail of microbial traces we leave behind us, as well as those we pick up from our surroundings, can be used to help reconstruct a picture of a person's activities and movements, like where they walked, what objects they touched and what environments they have been in.

Monitoring your scent

Identifying people by smell is actually one of the oldest police tricks in the book, but doing it with computers instead of bloodhounds is still in its infancy in comparison with facial and fingerprint recognition. The field of odor biometrics may be useful for individual authentication but is not well suited to mass surveillance – separating exactly who smells like that in a crowd can be tricky, as anyone who has been stuck in public transport on a hot day probably knows.

Bum detection

Then there are the identification techniques designed for very specific use cases. One pioneering suggestion from a team of Japanese researchers for an anti-theft system for cars was based on using 360 sensors to measure the unique shape of the driver's rear end. Despite achieving a 98 per cent accuracy rate in trials, tragically this important security innovation does not seem to have gone any further than lab testing.

The regulation problem

Trying to regulate surveillance technologies one by one is likely to be futile. The surveillance industry is simply developing too fast, and it is too easy to switch from one kind of surveillance to another. The difference between a facial recognition system and one based on behavioural biometrics may simply be a matter of swapping the software on an existing camera network, for example.

Increasing cooperation between government agencies and the private sector also means that regulations like San Francisco’s, which limits only government use of certain types of surveillance, are insufficient according to Katina Michael, a professor in the School for the Future of Innovation in Society and School of Computing, Informatics and Decision Systems Engineering at Arizona State University.

Amazon is perhaps the prime example for this blurring of the lines between private and government surveillance. Amazon has previously come under criticism for selling facial and emotion-recognition systems to police. More recently, it has been revealed that Amazon is partnering with hundreds of law enforcement agencies in the US, including giving them access to surveillance data gathered through its Ring home doorbell in return for police actively marketing the devices to the community.

"Fundamentally, we need to think about democracy-by-design principles," Michael says. "We just can't keep throwing technologies at problems without a clear roadmap ahead of their need and application. We need to assess the impact of these new technologies. There needs to be bidirectional communication with the public."

Surveillance changes the relationship between people and the spaces they live in. Sometimes, that change is for the better; there are real benefits from increased security, and the insights which can be gained into how people use public places can be used to help shape those places in the future. At the same time, however, we need to ask ourselves whether the future society we want to live in is one which constantly watches its citizens – or, more likely, one in which citizens are never totally sure when, how and by whom they're being watched.

Digital Society is a digital magazine exploring how technology is changing society. It's produced as a publishing partnership with Vontobel, but all content is editorially independent. **Visit Vontobel Impact** for more stories on how technology is shaping the future of society.

TOPICS DIGITAL SOCIETY WITH VONTOBEL SECURITY PRIVACY TECHNOLOGY

MORE FROM WIRED UK