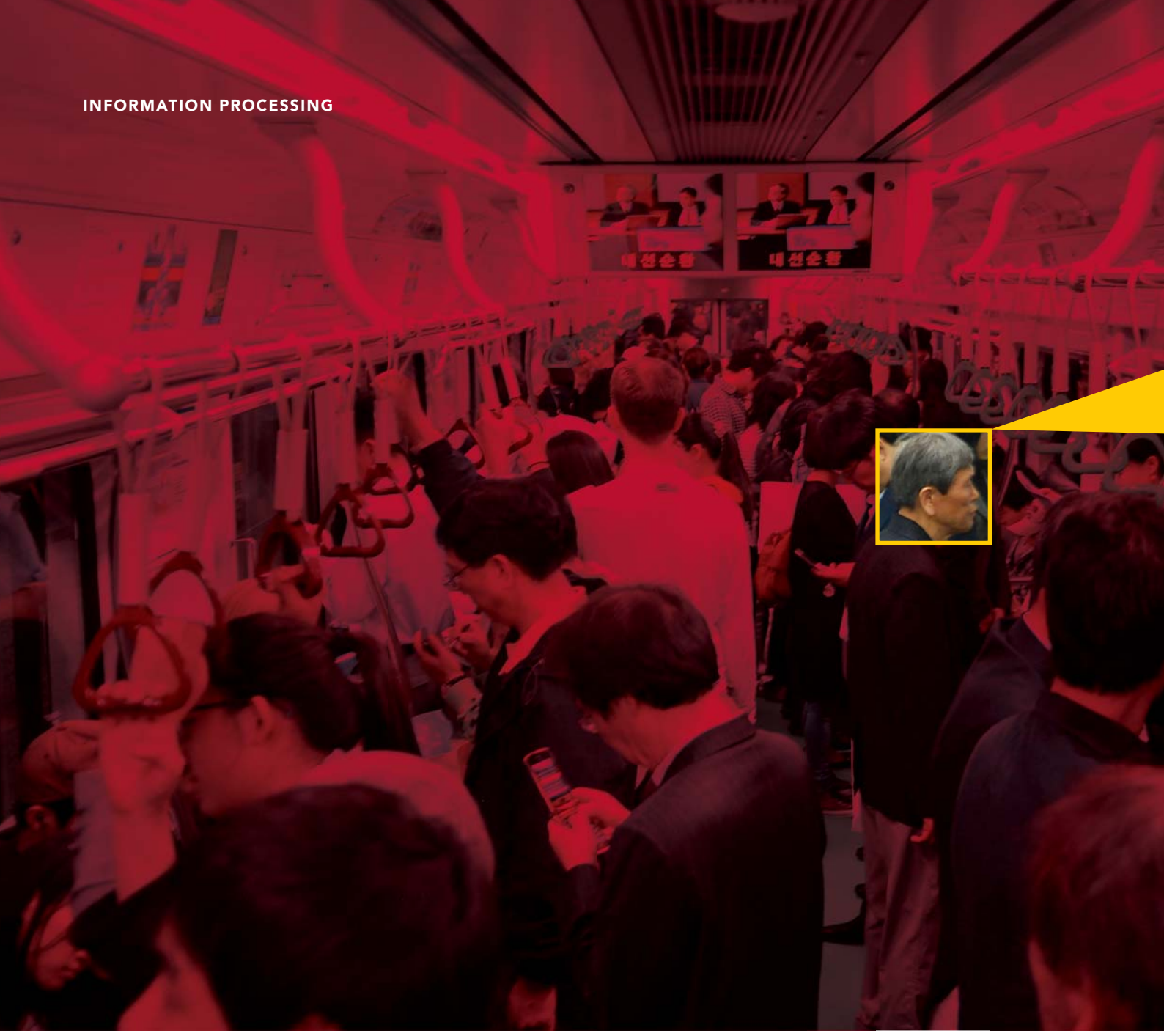

A FACE IN THE CROWD

REBECCA MERRETT LOOKS AT AN EXTREME EXAMPLE OF FAST-TRACK DATA PROCESSING: FINDING PEOPLE ON THE MOVE WHO MIGHT NOT WANT TO BE FOUND.

Terrorists can be a law-abiding bunch. They never jump the barriers at railway stations, preferring to buy their tickets and disappear into the crowd.

But can they?

Imagine processing massive amounts of video data from surveillance cameras and rapidly churning out usable and reliable information on pick-pockets, drunken hooligans, criminals or, yes, terrorists. Can authorities track a suspect individual across their journey among a myriad of other people, processing complex data in real time so they know where someone is, or at least has been?

Picture this: The London Underground (the 'Tube') carries 4 million passengers a day. These passengers can arrive at any one of the network's 270 stations, change to any of the 11 lines and other stations at will, and leave by another station (or even the one they entered the network by) with complete autonomy and impunity.

Monitoring this movement of millions are 12,000 surveillance cameras, each potentially sending data every second of every day. Manually tracking just one individual under these conditions – allowing for varying lighting, crowded platforms and all based around a few pixels on a video image – is a lengthy and frustrating experience. Tracking several individuals through different journeys just exponentially compounds the issues.

Where to start, where to continue looking, and all that assumes you know who you are looking for.

This is what Michael Haddy, CEO of Adelaide-based software engineering company Innovation Science, took on with his Rapid Passenger Tracking software.

The patented capabilities of the tracking software can automatically process masses of raw video data, locate the relevant footage and provide a short list of suspects within seconds of reporting an incident.

"The data reduction step just takes a couple of seconds so it's very quick to get to the set of surveillance video and data out of the network that then requires analysis," Haddy says.

"We very quickly identify groups of people within our suspect list and then provide those to the operator, and that would be reducing a million people in the network down to just a handful of groups."

Ticket fraud on the Tube is extremely low, so the vast majority of people, even those planning a crime, carry a legitimate ticket. Tickets passing through entry and exit turnstiles represent a largely untapped security infrastructure. Although they can be supplemented by other technologies to counter the less scrupulous traveller, ticket transactions provide an ideal indication of when and where the vast majority of individuals enter or exit the rail network. Ticket transactions therefore contribute basic intelligence that can support more complex analysis tasks.

The tracking software pinpoints where and when suspects have been throughout their journeys, from entering the network to arriving at the crime location to exiting the network. It can also determine if different suspects could have feasibly been in contact with each other during their journey and where and when that could have taken place.

Haddy points out using facial recognition technology alone to filter through that amount of passengers would not be practical, especially when aiming to capture information on suspects quickly.

"The problem is when cameras have low light or are positioned in low

light conditions and it's in a crowded environment it's pretty impossible. Even if facial recognition is possible in those sorts of conditions, the amount of computing power required to track millions of passengers would be prohibitive.

"The Rapid Passenger Tracking solution basically uses facial recognition – whether that's by a human, or a computer, or a combination of the two – only in the very last step in our processing chain after we've reduced the problem to a manageable data set."

Using the 2005 London bombings as an example of how crucial quick detection is in subway crimes, Haddy says it took more than a week for investigators to manually locate video showing the key suspects at King's Cross station which subsequently proved critical to the investigation. The search of video data at King's Cross was a result of "somebody's hunch". Based on various scenario tests in simulation environments created for the London Underground and other networks around the world, he believes the tracking software would be able to isolate video of the bombing suspects within minutes and have allowed investigators to examine complete journeys for suspects the same day.

In fact, it was the 2005 bombings that originally inspired Haddy to develop his system. He says he was sitting on a plane flying between London and New York when, instead of reading the usual airport novel, he began tapping out elaborate graph theory algorithms on his laptop.

The tracking software automatically discards video footage of passengers who are irrelevant to an investigation. This not only helps protect the privacy of those passengers not involved in a crime incident, but also helps deal with network bandwidth constraints by reducing the amount of video data that's needed to download or retrieve.

Although the names and addresses of most passengers will not be known, the software will identify where and when each relevant passenger entered the network, how they got to the incident, and an image that can be used for facial recognition and, in the case of very serious incidents, for police call-centre and casualty management.

"It determines which passengers are relevant to any incident and retrieves an image or video of those specific passengers from surveillance footage captured when they enter or exit the rail network. This will generally be a tiny fraction of the million or so passengers that would be travelling on the network at the time of a peak-hour incident," Haddy says.

"It then isolates snippets of video from the entire surveillance camera network that are highly likely to contain images of those relevant passengers throughout their individual journeys – irrespective of where the incident itself is located. The vast majority of surveillance video is discarded as soon as the software determines that it is irrelevant to a particular incident. It is then realistic for automatic and semi-automatic processing to be performed on the remaining surveillance video footage to prove each relevant passenger's whereabouts throughout their entire journeys."

Haddy says correlation of results generated by the tracking software has yielded some "useful 'every-day' crime fighting benefits" such as detecting pick-pocketing incidents which are considered to be low-end crime but "have a significant effect on the public's perception of a rail network's safety".

Low value crimes such as pick-pocketing are the most common crimes to occur on most rail networks. Limited police resources mean that they often go un-investigated. The new system will go some way to rectifying this situation.

"It takes just a few seconds to tell the passenger tracking software about each pick-pocketing incident. The tracking software then automatically correlates similar incidents. Once certain thresholds are met, the software notifies transit police by presenting photographs of individuals who are believed to be likely pick-pockets. Human surveillance resources can then be directed to these suspects when the suspects are next detected entering the rail network," he says.

Haddy says the correlation capabilities of the technology show considerable potential and there are more possibilities to explore or to further advance in this area in future.

Admittedly, the software relies on a train network being complex and, ideally, having a ticketing system that registers entry and exit movements through its turnstile infrastructure. This makes it ideal for cities such as London, Seoul and Hong Kong. Local Australian rail systems may be less likely candidates for its use, either because they require significant additional security infrastructure or because the transport networks themselves are not sufficiently interconnected. But where the infrastructure is in place and the network is complex, then such networks are likely candidates for a solution that helps detect and sometimes even solve or prevent incidents and crime.

"There are certainly lots you can do with correlation of the data that the system extracts," Haddy says, "so it's possible that we could automatically correlate certain information more than we do at the moment."

> "The data reduction step just takes a couple of seconds so it's very quick to get to the set of surveillance video and data out of the network that then requires analysis"

Missing that airport novel might end up being an extremely valuable contribution to transport security, and data processing generally.