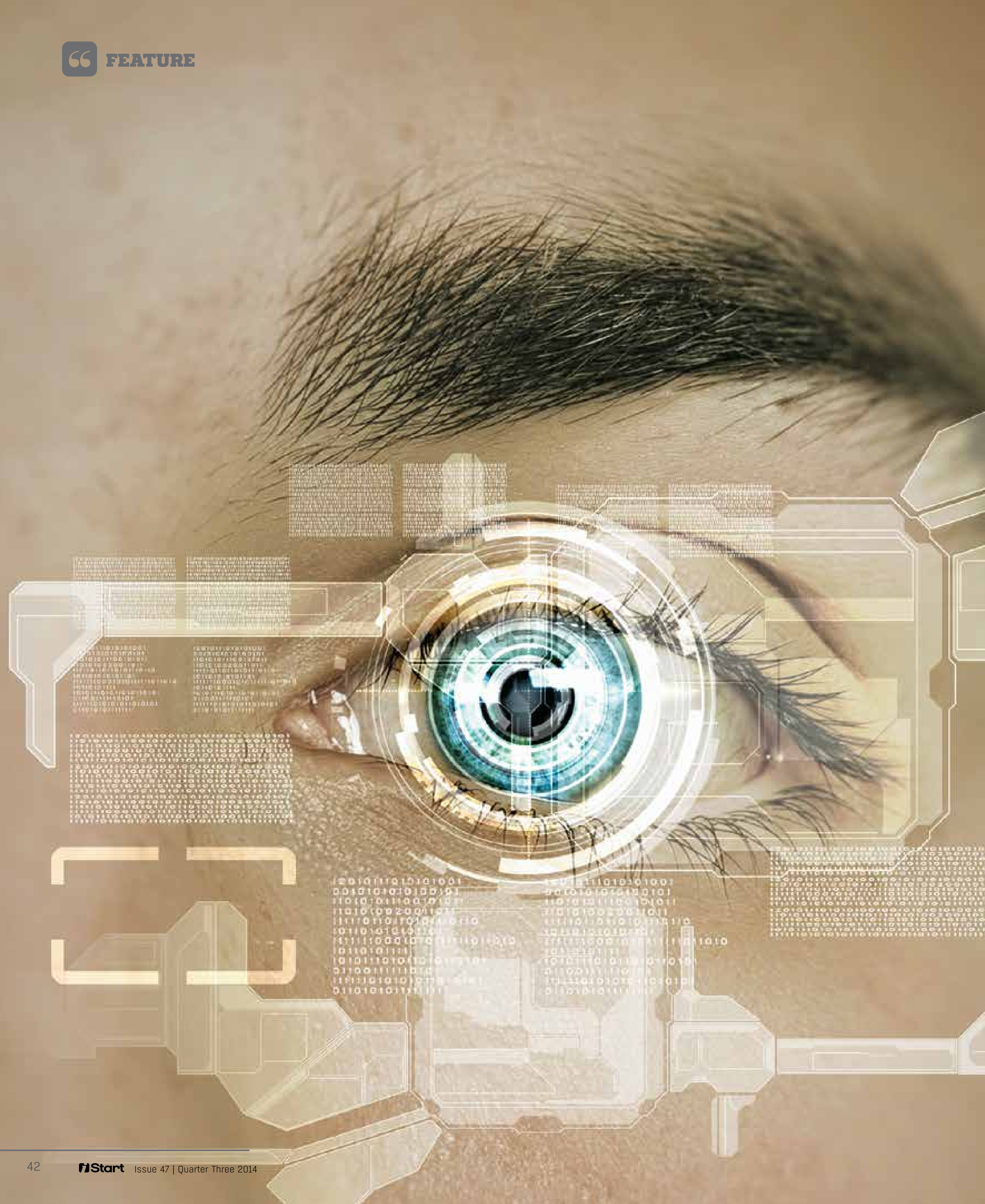

# SCANNING THE BIOMETRICS MARKET

*Security analytics, biometrics and behaviourmetrics all seem kind of Doctor Spocky, but they are rapidly migrating from sci-fi movies into the real world.* **Clare Coulson** *looks at what is possible in the complex world of security and crime prevention, and what is being used to protect us – whether we like it or not...*

"The FBI has been in the biometric business nearly a century." That's according to the FBI's senior technologist of the science and technology branch, James Loudermilk, who recently spoke at an international biometrics conference about the bureau's latest updates to its biometrics programme. While we tend to think of biometrics as being the height of whizz-bang technology à la Hollywood and CBS, fingerprinting for identification purposes has been in practice since the 19th century. According to the FBI's website its Information Division was established in 1921 by an act of Congress to be a national repository of law enforcement fingerprint records. Today, as Loudermilk explained at the conference, the bureau's current automated fingerprint identification system is in the midst of being upgraded to the faster 'Next Generation Identification' (NGI) Program – a 'multi-modal' biometric data repository that not only holds fingerprints, but corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and known aliases. The NGI Program isn't due for completion until later this year but Loudermilk says that as of autumn last year it already had a searchable dataset of more than 17 million legally-collected facial images.

The reasons for the upgrade are outlined on the bureau's website, where it says the future of identification systems is progressing beyond the dependency of a unimodal biometric identifier towards multimodal biometrics and the NGI Program will advance the integration and indexing of additional biometric data that will be required by a multimodal system.

A biometric system that relies on measuring a single biometric trait is said to be 'unimodal' while a biometric system that measures several biometric traits is 'multimodal', explains Gartner analyst Anne Elizabeth Robins in her paper *'Applying Biometrics for User Authentication'*. She confirms the FBI's assertion that multimodal systems are the future of biometrics. "Today's biometric systems measure a broad range of biological and behavioural traits. These traits include fingerprints, iris structures, vein patterns of the retina, geometry of the hand, palm and fingers, geometry of the face, characteristics of selected locations of DNA, dynamics of typed keystrokes, dynamics of movement when signing, dynamics of gait when walking, and acoustics of the voice."

### THE ETHICS EQUATION

The New Zealand Data Futures Forum is a group of academic, private and public sector experts that has explored how New Zealand businesses, government, researchers, and the public can safely share data and use it to build a prosperous New Zealand. It has produced a discussion document that presents some principles to guide data users and gatherers in a constantly developing environment so that the benefits of data use and sharing can be realised safely.

The New Zealand Data Futures Forum says it is of the view that an approach that emphasises data use rather than data ownership will be better suited to dealing with these new, innovative developments and meeting some of the challenges.

The Forum proposes four principles for safely managing and optimising data use in New Zealand in the future – these are intended to guide solution development and ensure we are achieving the best outcomes in terms of harnessing the benefits and maintaining trust and protection:

1. Value – use data to drive economic and social value and create a competitive advantage.
2. Inclusion – all parts of society should have the opportunity to benefit from data use.
3. Trust – Data management in New Zealand should build trust and confidence in our institutions.
4. Control – Individuals should have greater control over the use of their personal data.

To find out more, visit www.nzdatafutures.org.nz

## On the market

The biometrics market is big but is rapidly growing bigger. Latest market data from Transparency Market Research indicates that the global biometrics market is expected to reach a value of $US23.3 billion by 2019 at a CAGR of 20.8% from 2013 to 2019.

The research says that increasing security concerns due to the rising terror attacks and crimes have created a need for high level security capability. In addition, the rising government initiatives such as e-passports, national identification programmes and various border control projects have helped to boost the market. The report identifies privacy concerns and the high cost of biometrics systems as constraints to future growth. It also highlights the increasing usage of multi-modal biometrics to enhance security levels, and says this is expected to create huge opportunities for this market in the upcoming years. North America accounted for 32.1 percent of the overall revenue share in 2012 but the Asia Pacific region is expected to grow at the fastest CAGR of 22 percent from 2013 to 2019, thanks to numerous evolving economies in this region including India, China, Australia, and Japan.

The report showed that the transport, visa, logistics and government segments together accounted for more than 50 percent of the overall biometrics technology market in 2012, due to the increasing need for examining traveller's credentials. As a result, it said it expects this end user segment to dominate others by 2019. Conversely, the increasing usage of internet banking for transactions, means biometrics technology is largely being deployed in the banking and finance sector and this segment is therefore expected to grow at the highest CAGR during the forecast period.

## Screening the screen

Biometrics has come a long way since its birth in the surveillance technology world. John Kendall, managing director of securities programmes for Unisys APAC, says it has gone from simple pattern recognition and reactive, after-the-fact analysis, to combining biometric trait readings with real-time analysis.

"In particular what we are seeing is that surveillance is now combining up with analytics and biometrics to do far more than it was ever able to do…. some of the more interesting things we are seeing now is video analytics doing behavior recognition," he says.

This is several steps further on from facial recognition, which has attracted a lot of press and is in use on the SmartGates at Australia and New Zealand's international airports. Behaviour recognition software identifies behaviours of interest, maybe suspicious behaviours, and is becoming increasingly widespread in airports and high security facilities for doing things like perimeter intrusion, he says. The software scans multiple video feeds in real-time and can be programmed to send an alert if, for example, anything one metre-plus and human-shaped enters a particular area; or it can look for a human or vehicle loitering or tailgating; for unattended or removed objects; for vehicles going in the wrong direction or too fast; and so on.

"Those types of automated behavior recognition are in real-time, so basically rather than having someone stare at the feed to figure out when something suspicious is happening, an alert will go out and automatically show the feed where that suspicious behavior is happening, so you can decide whether activity is required or not. That's a lot more useful than the guy with his coffee mug and feet up on the desk staring at the screens," says Kendall.

The software can be integrated with other business systems and can even identify the type of threat and alert the people with the right skills to deal with it on their mobile devices, while informing head office of its actions.

## Voice your approval

As Loudermilk said in his recent speech at the IBIA, a lot of work is being done in the area of voice biometrics, which he called one of the oldest automated biometrics, dating back to the 1940s. "A tremendous amount is being done with speech today and it's very important."

The popularity of voice biometrics research is likely being driven by the demand for internet and mobile banking, noted in the Transparency Market Research report.

Joshua Feast, CEO and president of Cogito Corporation, which specialises in voice biometrics and has a product that gives callers real-time feedback on the progress of their conversation, explains: "At the moment the way that businesses are using voice biometrics is to a) secure transactions and b) to make sure that the person who is doing it is actually authorised to do so."

Michael Steinman, director of technology for another voice biometrics company, Nuance Asia Pacific, says research shows that 80-90 percent of people typing a password into their phone make mistakes and it's frustrating. Banks, enabled by the ubiquitous presence of microphones on smartphones, are therefore moving towards voice authorisation via the phone to help fight fraud and offer a seamless experience across all devices. "Your voice print is unique so the phrase doesn't need to be," he says, adding that passwords and

PINs are really not secure.

Voice identification is based on the underlying physiological characteristics of the speaker's voice tract, not on behavioral characteristics like accent or emotion so speakers are identifiable even when under stress or attempting to disguise their voice. The next step for voice biometrics, however, is trying to understand psychological state. For example, Feast says, how can you automatically tell if someone is trustworthy? And, to take it further in to the realm of behaviourmetrics, how can you use the 'self as a sensor', which analyses involuntarily reactions, to help understand situations more implicitly?

## In business

In April this year a report by Gartner asked '*Are Mobile Biometrics Ready for the Enterprise?*'. The report authors, Anne Elizabeth Robins and Trent Henry, came to the conclusion that although options for using mobile biometric technologies for user authentication are increasingly available, this availability doesn't necessarily mean they are viable for enterprise use. Many biometric solutions still lack maturity, and most don't yet meet the end-to-end requirements for a robust enterprise authentication solution. Added to this, most enterprises are not yet willing (or, in some cases, able) to adopt these new solutions, and so default back to more traditional, even if less intrinsically secure options.

Robins and Henry recommend that enterprises that are not yet ready watch competitors in their industry to get an idea of a roadmap, and consider doing small-scale pilots using cloud-based solutions. For those who are ready, they recommend amongst other things choosing a proven and accessible biometric mode and addressing privacy and compliance issues "early and often".

## Future projections

Feast says there is a lot more to come in the biometrics market. "It's a very immature market I think – it's been around for a long time but it's only really reasonably recently [in the last five years] that we've started to get good results collectively as an industry."

He says one of the biggest problems for business is "insights versus interventions". In his early days at Cogito they used to generate reports and tell clients which of their customers needed more attention but that required their clients to go away and spend money to do something about it. Today, he says the best technologies are ones that have both insight and intervention so users get the benefits just by deploying the solution.

And, it goes without saying, that you need to figure out what you are trying to achieve. "We understand these technologies can be used for all sorts of things, but it's not always appropriate that they be used because you start getting to the point where it is an invasion of privacy," warns Kendall. "Are there other, less intrusive ways to achieve the same result?" he asks.