



# PROFILING THE CRIMINALS

IMAGE DATABASES WILL BE MASHED UP WITH CRIME DATABASES TO FORM THE ULTIMATE VIEW OF CRIMINAL SOCIETY, REPORTS JOSHUA GLIDDON.

■ A decade ago, following the September 11, 2001 attack on the World Trade Center in New York, Boston Airport put in place face recognition technologies in a bid to track potential terrorists.

A public outcry put paid to those efforts, but technology has come a long way in the intervening years.

Today, Facebook will automatically tag photos with its best guess as to who is in them. If the authorities tried to create a universal database of facial images, there would be hell to pay. What's actually happened is that we have done it all ourselves, no questions asked.

"Biometrics is evolving to the point where we can take the image on a driver's license – and that's a pretty low res scan – and use that to obtain high quality face recognition matches in a database," says David Chadwick, law enforcement lead for systems integrator Unisys.

"Iris technology – iris scanning on the move – where you can get a match from several metres away, has come along in leaps and bounds and even the humble fingerprint is subject to much higher

resolutions than were ever possible in the past," adds Chadwick, who also happens to be a former police officer.

## FACE TRACKING

The reality is that biometrics is all around us, and we've come to accept it, generally speaking, as something that is universally good. It enables fast-tracking at airports, allows access control to sensitive sites and, of course, has significant implications for criminal and law enforcement.

"Facebook has definitely caused some concern," Chadwick says.

"The question is where does the biometrics used in social media go from here? Where is it going to take us in the future?"

One area of concern, currently under investigation by former NSW Police Commissioner Mick Keelty, is the impact social media has on covert police investigations.

There are two aspects to this. The first is that in future, it's reasonable to expect all prospective law enforcement officers

will have some sort of social media profile from their days at school and in university and post-graduate studies. If, as is currently possible, criminal elements are able to take a picture of someone, and then use social media biometrics to identify that undercover individual, where does that leave covert law enforcement?

The flipside is if someone has a covert identity established for them to enable them to undertake undercover work. If their criminal associates then run social media biometric backgrounders on them, and there is nothing there, then the viability of that undercover identity is again called into question.

At present, there's no easy answer to these questions.

## PLOTTING THE MAPS

One of the central aspects of law enforcement software is the fact that there is no central "do it all" application that acts as a crime dashboard for law enforcement professionals. Several companies are working at creating such a

**“LAW ENFORCEMENT OFFICERS DON'T HAVE THE TIME TO UNDERTAKE EXTENSIVE TRAINING IN A NEW PRODUCT – THEIR FOCUS IS OBVIOUSLY ON MAKING SURE THAT THEY ARE OUT THERE ENFORCING THE LAW. USERS CAN BE UP AND RUNNING WITHIN A DAY.”**

**SOUTH AUSTRALIA'S CITY OF PROSPECT**

enforcement agencies. Private enterprise and government have also become big users of the software.

Broadbent says there are no reference sites for policing in Australia for the software, but says local government has become a big user, particularly in the fight against graffiti crime.

“Graffiti costs local governments around quarter of a billion dollars every year across Australia,” he explains.

Brisbane City Council invested in the software, and has become one of the biggest users in Australia. Its use of the software, which is used to plot graffiti outbreaks (and to record the tags used by graffiti criminals) has led to a direct drop in graffiti crime because local police can be easily directed to graffiti hotspots. By directing law enforcement to hotspots, patrols can be increased and known graffiti criminals profiled by their tags.

“The thing is that the product needs to be simple,” says Broadbent. “Law enforcement officers don't have the time to undertake extensive training in a new product – their focus is obviously on making sure that they are out there enforcing the law. Users can be up and running within a day.”

Broadbent also points to several other jurisdictions' use of the software as a crime fighting tool. British Telecom uses it to track theft of copper from its network.

“Once copper was seen as a cheap metal. No one wanted it,” he says. “Now it's valuable, and gangs go about stealing it from telecommunications companies' networks, with all sorts of knock-on effects for the company and its customers. Not to mention that replacing the network is also expensive.

“Using Crime Profiler, they are able to identify hotspots for copper theft, see it on a map, and direct law enforcement towards it,” Broadbent says.

### ANALYSING THE DATA

SAS is a company well-known for its strength in data analysis. It recently purchased British company Memex in a bid to strengthen its presence in the growing law enforcement space.

One of the challenges for modern police forces is the sheer volume of data available to them. There are incident reports, images from crime scenes and also video from fixed cameras. Then there are data from seemingly unrelated areas, such as tax and income, along with other unstructured data sets.

SAS's software allows law enforcement to drill down into pools of data to find connections that would not be apparent on the first, or even second pass, even for experienced crime analysts.

“We have married operational

intelligence with data intelligence,” notes SAS general manager for risk intelligence, Brendon Smyth.

“The question law enforcement must constantly deal with, is when you are looking at huge amounts of data coming at you, how do you deal with, and make sense of it all?” he asks.

“The sky is the limit in terms of what this software can do, and also in terms of the volume of data that it can handle.

“It's especially relevant in terms of the move towards fusion analytics, and the creation of fusion centres to analyse broad swathes of data from disparate sources.”

### THE MOVE TOWARDS FUSION

The Australian Crime Commission (ACC) last year established its Fusion Centre with \$14.5 million in funding from the federal government. So far it has uncovered 53 new targets in serious organised crime, and generated 2300 new actionable leads, according to figures supplied by the ACC.

The ACC brings together data from law enforcement, tax and other data sources, and then applies data mining techniques to the information to draw associations between the seemingly unconnected information sources.

“What we have created in the first 12 months is pretty unique in terms of what we have seen in North America and Europe,” ACC acting executive director David Lacy told *The Australian* newspaper.

“That's one of our roles, but because of the role of the ACC, particularly in proactively identifying organised crime and monitoring it, there's a secondary and, I think, higher-order opportunity and priority for us, and that is more around generating, proactively, targets previously unknown for the jurisdictions to support those agencies,” he says.

### POWERFUL SOLUTIONS

Law enforcement still lacks a panopticon-like view of crime throughout its jurisdiction.

But make no mistake, because it is coming.

NSW Police has a powerful image-matching database.

Facebook knows who you are, and your local council is pulling out all stops to put an end to graffiti crime.

Soon enough, image databases will be mashed up with crime databases to form the ultimate view of criminal society.

Until then, there are plenty of powerful solutions on the market to help both public law enforcement and private companies fight crime on their turf. Those solutions are only going to get more powerful as computing power increases over time. **GN**

dashboard, which will take into account all the reported crime in an area and overlay that data onto mapping software.

One of the leaders in the field is Pitney Bowes, with its product Mapinfo Professional Crime Profiler.

Ian Broadbent is the manager for policing and public safety, EMEA, at Pitney Bowes. He's also a former police officer with Manchester police service, in the UK, where he oversaw the use of mapping software to fight crime.

“What this software does is that it automates the crime profiler's work,” says Broadbent. “It looks at the density of the crimes in a given area, and estimates whether the locations means that there are any links between them.”

The second aspect of the software is the dashboard application which enables the crime analyst to pump into the system data about crime incidents, their density and location, and then produce graphical representation of the crime.

One of the most interesting aspects of the Crime Profiler software is the fact that it's not just used by law