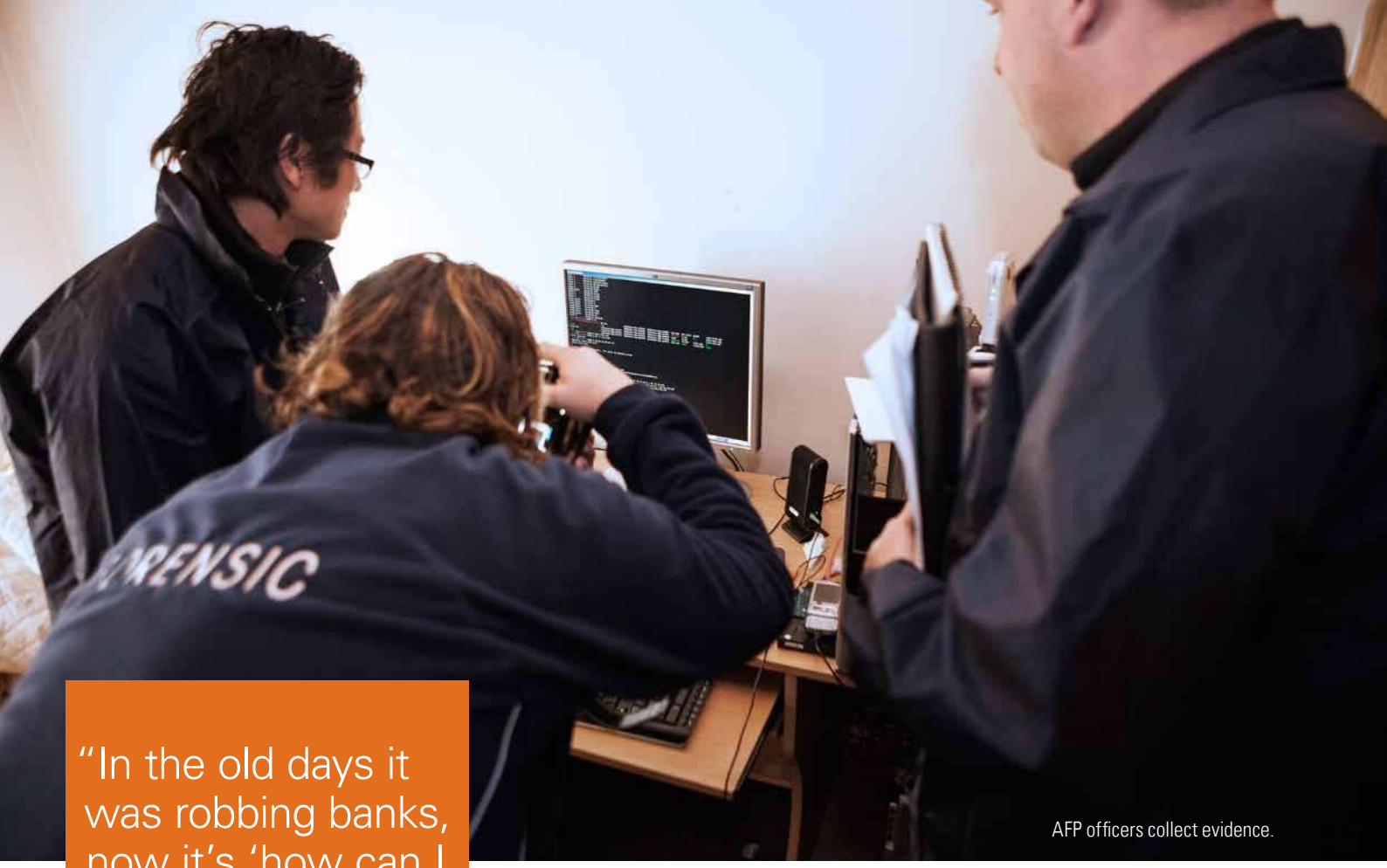
Call disconnected

Telecommunications data retention is a critical issue for law enforcement to prosecute serious criminals and the public needs to know the issues.



AFP officers collect evidence.

"In the old days it was robbing banks, now it's 'how can I access information that I can monetise'

The rise of the digital age has changed lots of things. Even language itself has not been spared the relentless march of the digital revolution. For the most part the average person can simply enjoy the fantastic advantages of hopping onto the cyber highway.

Yet, the digital age is no respecter of tradition. The industrial age has taken a lot of hits. Retail outlets, banking, venerable media agencies – all people have felt the sting of digital innovation as the 'rivers of gold' run online and go global. Does anyone remember where their local video store used to be?

Law enforcement agencies and the business of catching criminals also has been blurred by the digital age. Crimes now more easily cross international boundaries. An offender may well be downloading child pornography in Australia, while the Internet Service Provider (ISP) they use is overseas. Furthermore, the data storage may well be outsourced to a third party in another country. Yes, it's complicated.

In fact, the digital age offers as many potential advantages to criminals as it does to the average person and law enforcement. For example, turning up at a bank with a sawn-off shotgun and balaclava in broad daylight is a risky business. Attacking the digital records of financial institutions and citizens is a much safer and more lucrative option for criminals.

"I could arguably be sitting in my bedroom in Belarus in my pyjamas and be attacking a bank in Sydney or Melbourne and emptying the bank accounts," says National Manager High Tech Crime Operations, Tim Morris.

"In the old days it was robbing banks, now it's 'how can I access information that I can monetise'? Sometimes it might be through various steps, but information is valuable to someone especially when they can monetise it. The simplest concept is credit card data. For instance, I can steal the credit card numbers and names and expiry dates and I can monetise that very easily."

Creating legislation that can keep pace with this level of constant change is problematic. The current review of the *Telecommunications Interception and Access Act 1979* (TIA Act) is a perfect example of how the transition from an industrial world to the digital age is, well – complicated.

The Act was drafted in the days when Telecom was Australia's sole telecommunications company (telco), landlines were in practically every home and sentinel-like phone boxes dotted city, suburbs and country towns alike. Back in those days, every phone call made left a trace or footprint that when necessary could be used to assist investigations. The concept that Australian families would soon have six international communications devices connected to their own wireless comms network was like some bizarre science fiction story.

The outcome of the TIA Act review is a critical concern for law enforcement agencies in Australia. It is not an overstatement to say that it could fundamentally hobble police agencies in fighting crime.

Metadata

The TIA Act outlines the criteria under which government agencies can access a communications network or device in the course of lawful duties. An important component of the Act deals with what has come to be known as metadata in the digital age. Metadata is basically what used to be known as 'call charge records'.

As the name implies, the call records of each landline were captured and stored by telcos in order to bill customers when they accessed the service. The telcos needed information such as when, how long and over what distance the phone call was made – and importantly, from and to whom the call was made. Essentially, it was in their commercial interest to keep the information so they could bill the customer.

Call records also are still extremely important to police investigations when approaching an offence in retrospect. Even if it was just to establish that Suspect A talked to Suspect B at a certain time on a certain date and at a certain location. These call records are still a primary means of establishing an investigation and attributing an action to an individual.

It was not an actual recording of the content of the phone call. Other criteria for a warrant apply when police believe there is justification to intercept a communication device in a current investigation. Call records were simply the administrative log entries of each phone call made.

The digital problem is that landline phones in homes and public spaces have almost disappeared faster than video stores. A report by the Australian Communications and Media Authority in 2013 states home fixed-line use dropped as Australia's most used communication tool from 22 per cent in 2012 to 16 per cent in 2013. In short, call records are diminishing as a dependable crime-fighting resource.

Telcos already store less reliable data in the digital age and for shorter periods of time depending on phone plans. A big frustration for law enforcement comes in the form of unreliable information held for pre-paid phones.

As the business need for maintaining metadata diminishes, so too is the data that police are retrieving on criminal suspects across all crime types.

Even so, the big difference now is that ISPs and telcos may charge only for the amount of data an individual uses. They don't need to know who a person is contacting. So long as the user keeps paying the monthly contract rate then the ISP or carrier keeps the service connected. There is no need for the ISP to keep and store extensive data records. Essentially, it's not in an ISP's commercial interests and so the valuable footprint left by communications is being lost.

The problem has compounded with the emergence of voice-over-the-internet protocols and smartphones. An individual can download any number of free phone applications, many of which are encrypted, and chat to anyone in the world over the internet for the price of the data usage. Unless metadata records are kept then this valuable source of information vanishes into the ether almost immediately.

When the National Broadband Network is completed, communications will be exclusively transmitted through digital data. As the business need for maintaining metadata diminishes, so too is the data that police are retrieving on criminal suspects across all crime types. Police are losing a fundamental building block for criminal investigations.

"I can hardly think of one investigation that doesn't include some cyber related aspect to it," Assistant Commissioner Morris says. "Even a telephone communication, an SMS, an email, a chat book log, what have you – from murder to kidnapping to drug importing to money laundering. You name it, there seems to be some sort of technology aspect to virtually everything we do."

Without a commercial imperative to retain the metadata, police are looking to legislation to guarantee the retention of metadata. That's why the TIA Act review is such a concern. It's hard to imagine that most people would have an issue with police catching serious criminals. But the public debate on privacy issues in the digital world changed drastically in 2013.

Computer technology is seized during an operation.

Edward Snowden has impacted the debate on metadata.

Edward Snowden

Edward Snowden is a computer systems and telecommunications specialist who, in short, worked very deeply inside the US intelligence world for several years. Snowden's significance is that in May 2013 he disclosed, in some estimates, more than a million classified documents to media outlets from his years as an intelligence insider. The leaks revealed numerous intelligence programs, tools and techniques used by US and other international intelligence agencies, including Australia.

Depending on one's world view, Snowden has been called everything from a hero to a traitor. But the problem with the Snowden revelations is that it has clouded significant democratic issues. The debate over public privacy and covert surveillance by governments is unfolding across the world in the wake of Edward Snowden's release of documents. Assistant Commissioner Morris says it is confusing the public debate in Australia just as the TIA Act is due for review.

"Unfortunately, the police have also been caught up in this debate and I would argue a little bit unfairly. There are some real differences between how the intelligence agencies are legislated, governed and overseen that are very distinct to the police's philosophical approach to intelligence led policing and investigations. There are fundamental differences that make the comparison not really a meaningful one."

Privacy vs anonymity

Snowden initiated an international debate on just how far governments should intrude into the privacy of individual citizens. The AFP submission to the TIA Act review wholly supports protection of privacy. But the submission urges that the AFP considers "… it timely to review the TIA Act and ensure that it remains an effective tool for law enforcement".

Assistant Commissioner Morris says there is a distinct difference between a person's right to privacy and a right to remain anonymous – especially

Former Director General of Security ASIO David Irvine and the AFP Deputy Commissioner National Security (now Commissioner) Andrew Colvin meet the media to explain the proposed new policy to retain metadata.

'We are not interested in people per se; we are interested in suspected criminals who engage in a whole wide range of unlawful activities in this digital space...'

when an offence is committed. He says the open and transparent lawful processes used by police in Australia to access metadata have little to do with privacy issues.

"We don't want to know who most people are," Assistant Commissioner Morris says. "We are only interested in people whose conduct is deemed unlawful. We are not interested in people per se; we are interested in suspected criminals who engage in a whole wide range of unlawful activities in this digital space – from terrorism, theft and child molestation to selling child pornography. They are the people we are interested in."

Assistant Commissioner Morris cites number plates as the perfect example. He says registration plates ensure privacy. "It doesn't have your name, address and date of birth on the registration plate," he says. "So you are afforded privacy. But if you are suspected of committing an unlawful act like a hit and run then there's an easy point for the police to ascertain who the driver of the car was. We can attribute the car to the person.

"So, yes, the AFP believes everyone has a right to privacy – particularly in the online environment. We do not have an argument. But do you have a right to anonymity, especially for unlawful purposes? We would argue not."

Conclusion

Assistant Commissioner Morris sympathises with legislators. He says law makers have the responsibility of keeping the community safe, while needing to manage the intrusion into people's privacy.

"In liberal democratic societies like ours, it is always going to be a contest between getting privacy issues balanced with access issues," he says. "It's a difficult job for legislators to get that balance right because public sentiment changes. It's not a constant."

Even so, Assistant Commissioner Morris says the AFP is not looking for an increase in powers under the TIA Act review. He says the AFP submission continues to support the "necessarily rigorous" provisions where only an authorised agency can intercept or access information. Rather, it is an opportunity to update the legislation to accommodate a new world.

The AFP submission itself states: "Much like the inflationary increase in the general price of goods and services in an economy leads to a reduction in buying power for consumers, the exponential changes to the telecommunications landscape has reduced the ability of agencies to effectively undertake lawful interception in the way intended by legislation. Reform is not a bid for more powers but an attempt to maintain existing capability in an increasingly complex environment."