BUILDING RESILIENT SOCIETIES
FORGING GLOBAL PARTNERSHIPS.
Edited by Susan Sim
BUILDING RESILIENT SOCIETIES.
FORGING GLOBAL PARTNERSHIPS.

ESSAYS FROM THE
INTERNATIONAL CRIME PREVENTION CONFERENCE 2011

ORGANISED BY THE
NATIONAL CRIME PREVENTION COUNCIL

14 – 17 November 2011
Singapore

Edited by
Susan Sim
Chairman, Research Committee
National Crime Prevention Council

Design By SCORE Digital Media
16. CRIME PREVENTION, SOCIAL NETWORKING AND COVERT OPERATIONS

NICK O’ BRIEN & MICK KEELTY
The Challenge of Undercover Policing

Organised crime during the 1980s and 1990s in Australia and other countries resulted in the introduction of several crime prevention strategies through government policies aimed at improving certainty of a person’s identity. Money laundering of the proceeds of crime was often facilitated through multiple identities and taxation fraud. The 1990s through to the present day has seen the growth of terrorism around the globe. Strategies introduced to be more effective in dealing with this crime type included undercover policing and operations using police with “assumed identities” obtained lawfully.

This type of covert operation by police required new legislation, at both State and Federal level, to allow police to legally adopt a false identity.

Infiltrating organised crime groups using a false identity and enticing criminals to turn against their co-accused and give evidence for the prosecution are very effective methodologies. These tactics can reduce the cost of prosecutions by providing compelling admissible evidence from witnesses who are agents of the prosecution.

Moves were also made to require higher degrees of scrutiny to verify identity documents to reduce fraud. Reducing the opportunity for multiple identities, fraud against the government revenue through the introduction of photographic licences, tax file numbers and social security identification became a priority for the government. The undercover police were inadvertently caught up in the system that required a legislative framework to enable them to verify their “false identity”.

These crime reduction strategies were supplemented by the introduction of sophisticated “witness protection” programmes.

These methodologies require the covert operative or the protected witness, to remain unable to be identified by organised crime or terrorist groups for the rest of their lives. Various strategies have been used in the case of police, to ensure that their identity is never known to the criminal element.

Sometimes, new police recruits, not yet exposed to criminals or terrorists are engaged as undercover operatives. The idea is premised on the fact that these “new police” are not yet known to criminal elements and this genre of police officer is less likely to have been exposed to the perils of corruption. Corruption is considered an enabler for some forms of organised crime.

Another strategy has been to use trained undercover police from other police forces either interstate or overseas, who are not known in the jurisdiction where the undercover operation is to be conducted.

In the case of a witness protection matter, it is possible that the person has already been part of an organised crime gang and may have lived and worked with the accused so masking their identity is problematic. Witnesses for the prosecution requiring to be ‘hidden’ from their jurisdictions have often found themselves in another part of the country or indeed, placed overseas until they are required to give evidence after which they are ‘resettled’ in another place and encouraged to get on with their lives with a new ‘assumed identity’.

This type of strategy to infiltrate crime or terrorist groups is extremely expensive. A UK undercover officer revealed in 2011 that the cost per annum for each officer was in the region of UKP 250,000 per annum (Graham, 2011). It is also extraordinarily dangerous for the individuals should they be discovered as being an ‘agent for the prosecution’. Equally, the families of these agents could be at risk should an agent’s true identity be discovered.
The Impact of New Media

The introduction of Social Networking Sites (SNS), particularly over the past five years since the introduction of Facebook has seen a change in social attitudes about what people keep private. The exponential growth of SNS has seen Facebook grow to over 800 million users as at December 2011. If it were a country, Facebook would be the third largest in the world behind China with a population in the region of 1.3 billion and India with a population in the region of 1.2 billion.

By way of example, out of 71.15% of all Singapore’s Internet users, 55.37% or over two and a half million are Facebook users. The profile of Singapore’s Facebook users is evenly split between males and females (Asia Marketing Research, Internet Usage, Population Statistics and Facebook Information, 2011).

The growth of SNS has seen a commensurate growth in the uploading of photographs to accompany social networking events. Facebook statistics estimate that up to 250 million photographs are uploaded onto Facebook every day, with a reported 750 million photographs being uploaded during the 2010/11 New Year weekend (Kincaid, 2011).

Given these developments, our research set about attempting to quantify the level of exposure of new police recruits at the time of embarking on their careers. The researchers were interested in the impact of the convergence of technologies in an environment where it is estimated that smart phones will outnumber other handsets by 2014 in Western Europe and will have captured 72% of that market by 2016 (Analysys Mason, 2011). Significantly, at the end of 2011, there were 6 billion mobile subscriptions with “smartphones showing the strongest growth” (Global mobile statistics 2012).

Added to the convergence of technologies, both facial recognition and photo tagging have become freely available. Access to cloud computing, thought to be new technology but in reality, simply a new term for old technology where banks of computers are pooled together to provide extra computing power will make cross referencing and searching of photos and facial features accessible to many more people, including organised crime.

The capability to search so many images can be facilitated by purchasing computing power from service providers such as Amazon Web Services, which provides capacity on a “pay by hour” basis (Amazon Elastic Compute Cloud, 2011).

In short, the researchers are attempting to find out whether we are witnessing the “death” of undercover policing and witness protection programmes used so effectively in the past three decades.
The Rise and Rise of Social Networking

Most observers would probably agree that the modern form of social networking commenced with the introduction of Facebook to the general public in 2006 (Kirkpatrick, 2010).

As of December 2011, Facebook reports that it has over 800 million active users. The story of Facebook has been the subject of several publications and even a movie, The Social Network released in 2010.

In January 2011, the President of the United States of America, made reference to Facebook in his annual State of the Union address. Indeed President Obama has even visited Facebook (Parr, 2011). Another example of the penetration of Facebook into our world was witnessed during the overthrow of the Mubarak Government in Egypt during the Arab Spring of 2011.

Another Arab country Libya, which also faced major civil unrest and the unseating and death of their controversial leader, Colonel Muammar Ghadaffi, was thought to be influenced by a civilian movement generated through social networking. This outcome was predicted in a speech delivered by Ghadaffi’s son, Seif Al-Islam Al-Qadhafi, at the peak of the Arab uprising in Egypt when he said, “Libya has oppositionists. They began to imitate what happened in Egypt, using the so-called Facebook Revolution”.

This raises the question as to whether Facebook or other SNS will in time have more influence then the ballot box in modern democracies.

It is interesting when you look at the globe and see the countries that have adopted Facebook as their preferred SNS. The maps below compare the take up rate of Facebook in 2009 with 2011.

Source: http://www.dailymail.co.uk/news/article-2003679/Amazing-maps-Facebook-taking-world.html
Of interest is the increased take up rate in South Asia, South East Asia and some African nations. Indonesia reportedly had nearly 39 million Facebook users in June 2011 which makes it the second largest Facebook user behind the United States. Indonesia’s Facebook penetration is nearly 16% of the eligible population.

Also of interest is the age profile of Facebook users in Singapore. Rather than being dominated by the younger generation, the largest user group at 32% of total users is aged between 25 years and 34 years. Nearly 60% of all users in Singapore are aged between 18 years and 34 years. As discussed later in this paper, this cohort offers those planning crime prevention strategies with some unique opportunities to deliver positive benefits from social networking.
But other SNS options have emerged as well, such as Twitter, LinkedIn, Foursquare and now, Google+. The question arises as to who will dominate the market. Popular SNS such as MySpace may simply dominate the market for a few years and then seemingly disappear. Google+ has had an extraordinary take up rate since it burst onto the scene in mid-2011 with CEO Larry Page announcing in October 2011 that it had “passed the 40 million user mark”. Twitter has also been widely embraced; in September, it announced that it had 100 million active users. It is also possible to share images on Twitter through third party applications such as Twitpic. Twitter provides the quickest way of distributing information to a large numbers of people.

In today’s world, crowd sourcing, sometimes referred to as crowd journalism, will challenge operational police to maintain the security over their activities. For example, the capture of Osama Bin Laden was first revealed not by officials but on Twitter.

LinkedIn is another SNS that has attracted high growth levels. In November 2011, 135 million people were registered on LinkedIn across 200 countries. More than half of the people who have embraced LinkedIn are located outside the USA and in 2010, LinkedIn saw 2 billion searches carried out on its site and the company estimated that 2011 will see 4 billion searches on the LinkedIn platform.
**Convergence of Technologies**

As of November 2011 there were 3.5 billion mobile subscribers, which represents 77% of the world’s population. Mobile telephones now have photographic capabilities that are equal or in some cases surpass the pixel capacity of some cameras. 2012 saw the introduction of the first 41 megapixel camera phone (Segan, 2012).

Capturing images on mobile phones has become commonplace because of the ease and the quality of the technology, not to mention its mobility. The modern mobile phone or smart phone is also a computer enabling the rapid distribution of photographs around the globe. Iris scanning technology has now been used as part of security controls in border protection. Air travellers, for example, can use a Nexus pass rather than a passport to cross the USA/Canadian border. This involves an iris scan check (Nexus Iris Scan Locations, 2011).

The intricate structures of the iris have enabled iris scanning to become a key to biometric identification techniques. Some computers rely on a captured image of the eye to allow use of the computer instead of code words or fingerprints. Once an iris image is captured it lasts a lifetime.
**SURVEY ON EXPOSURE LEVEL OF 2010/2011 POLICE RECRUITS**

A survey instrument was developed and distributed to police recruits from two Australian police forces and three other Australian agencies that use covert operatives with access to assumed identities.

An introduction to the research was explained to the respondents and respondents retained their anonymity by individually accessing the survey instrument through a URL site established by Charles Sturt University. The Australian Democratic and Social Research Institute based at the Australian National University assisted in the analysis of the survey results. Survey respondents were not identified but their agency was made known to the researchers.

The survey established that 85% of respondents were using a Social Network Site, with Facebook being the most popular site. The percentage of people using social networking sites were much higher in younger age groups – over 90% for all age groups under 36 years – compared with a low of 45% for the 46-50 year age group.

47% of the survey respondents used a social networking site daily and another 24% used a site weekly with an even spread between male and female respondents. A higher percentage of younger people use social networking sites on a daily basis.

It was discovered that over 90% of the respondents aged 36 years or younger were using SNS. 85% of the respondents were aware that their photograph had been uploaded on the Internet by another person. Almost 100% of respondents aged 26 or younger knew that their photograph was available on the internet.

When the research was started in 2010, the only way to have your photograph removed from a Facebook entry was to seek the agreement of the person who uploaded the photograph. More recently, provision has been made for people to approach Facebook and have their photographs removed.

The survey sought to establish whether it was possible to identify a police recruit through his or her network of friends. In other words, if you were unsure whether someone was a police officer, could you establish that fact by searching his or her friends and acquaintances? 42% of respondents thought that it would be possible to identify their relationships with other people through the Internet.

21% of the respondents said it would be possible to associate their photo with their personal details on the Internet while a higher percentage, 36%, said that they did not know or had never checked. 16% said that they had considered the consequences of facial recognition software when uploading their photos on the Internet whereas 39% of the respondents had not considered the possibility.

37% did not answer this question, giving rise to the suggestion that while they were answering the survey questions, they may have realised the implications of captured images of them on the Internet as they were embarking upon their careers as police or intelligence officers.

Finally, 28% of the survey respondents answered that completing the survey had caused them to be concerned about their profile on the Internet (35% of females, 26% of males).

After the surveys were completed, the researchers began discussing the results with various academic groups, policy makers and others. In discussing the results with operational personnel, issues began to arise which may be considered incidental to the research but they highlight the challenges ahead for any type of secure operation.

For example, police will often delay briefing large numbers of officers about impending operational activity against high priority targets until the last
minute in order to maintain operational security and to maximize the impact. To mitigate the risk of exposure, specific details of the operation are retained by a small number of essential staff on a “need to know” basis. But often, there is a requirement for supplementary staff to be brought in to assist the operation. If the supplementary staff have a well-publicised profile on SNS or frequently use the geolocation feature on their Smartphone, operational security can be rapidly compromised.

**USING SOCIAL NETWORKING FOR LAW ENFORCEMENT**

In terms of crime prevention, it needs to be remembered that there is little or no authoritative way to ensure the true identity of entities on the Internet. There is no better recent example than the recent attempt to engage with the heads of defence and intelligence agencies by a group who pretended to be the head of NATO forces. Apparently “friend” requests from Supreme Allied Commander Admiral James Stavridis appeared on the Facebook sites of significant military and political personnel from the US, UK and allies. However, a newspaper has reported that the profile was created by “foreign spies” (Lewis, 2012).

While the focus of the research has been directed towards the ramifications of inadvertent (as opposed to deliberate) disclosure of a person’s identity when using a social network, there are some positive uses for law enforcement especially when it comes to the intelligence available from trawling through social networking sites.

Equally, recent natural disasters such as the Tsunami in Japan and large floods and cyclones in Queensland, Australia, have highlighted the value of social networking as a law enforcement tool for assisting the community.

In the Queensland flood example from early 2011, the use of Facebook grew exponentially as the disaster was being managed. Prior to the floods, Queensland had 1.4 million Facebook users. In December 2010, the Queensland Police had only 7,000 friends. This grew to 12,000 by January 10, 2011 and their Facebook page received 39 million hits. By the end of the disaster, Queensland Police had 172,000 friends and it is still growing today.

The Queensland Police established “Terms of Use” for their Facebook page and enabled information from the public to be authenticated and rebadged as a Queensland Police entry on the Facebook page. Some friends on Facebook were “black listed” by the police as they were putting false entries on the Facebook page. The police also used Twitter to keep on top of information being provided by the community and allowing it to be broadcast as an “official tweet”.

Facebook and other social networking sites have enormous capacity to process information. Queensland Police were able to present “live streaming” of flooded areas to warn the public about the dangers they were facing.

**CONCLUSION**

The growth in both the take up rate of these technologies and advances in the technologies themselves will have an impact upon the ability of anyone to remain anonymous or use an assumed identity.

This has an immediate impact upon the current practices used by undercover police and other national security activities that rely upon assumed identities.

There are other implications for law enforcement. Where a witness has been placed under witness protection and given a new identity, there is now a possibility that previous images of the person will be linked with his or her original name.

In countries where there are Occupational Health and Safety laws governing the obligation of employers to protect their workers from injury or harm, the convergence of technologies presents some immediate challenges. A failure
by employers to understand and recognise the advancement in these technologies could expose someone such as a Commissioner of Police to litigation for failing to protect his/her undercover police from being harmed.

New ways of achieving the same outcome as an undercover police officer will need to be implemented. The most obvious of these is the expanded use of human sources to obtain the intelligence and evidence required to provide vital evidence against organised crime.

The response to the loss of privacy was put to Google’s Executive Chairman Eric Schmidt, who said that you should change your name on your sites (Hearn, 2010). But of course, once a photo is tagged with your name, it is recorded forever. The facial recognition scan capability will ignore the name and present identical images of a person regardless of the name.

This research produced an interesting outcome on a question to the police recruits about whether or not the captured image of their face has given them a cause for concern. 45% of the respondents were not concerned. However, 37% of the respondents did not answer that question, giving rise to conjecture that while they were answering the survey questions, they may have realised the implications of captured images of them on the Internet as they were embarking on their new careers.

What is clear is that if our research at the beginning of 2011 showed that nearly 100% of police recruits aged 26 years or younger were already recorded on SNS, the embracement trends in social networking means that we may have seen the end of the ability of a person to take on an assumed identity for undercover police work or other type of covert operation. This research will continue to measure these trends but there is a need for undercover and covert operation strategies to be cognisant of these issues.

REFERENCES


