Issue 1, Number 2
2013

Salus Journal

A peer-reviewed, open access e-journal for topics concerning law enforcement, national security, and emergency services

Special Issue on Privatisation of Intelligence

Published by

Charles Sturt University

ISSN 2202-5677

Issue 1, Number 2

Published by
Charles Sturt University
Sydney, New South Wales, Australia

ISSN 2202-5677

Salus Journal

Issue 1, Number 2,
2013
Special Issue: Privatisation of Intelligence

Contents

Licensing

Editorial

THE PRIVATE WORLD OF INTELLIGENCE

Troy Whitford, BA, MA, PhD*
Hank Prunckun, BSc, MSocSc, PhD
Kate O'Donnell, BBus, MA, MCCJ(Hons)

Special Edition Editors

It has been argued that since the terrorist attacks of September 11, 2001, no other profession has experienced change to the same extent as that of intelligence. As evidence of this we have seen the profession grow in the number of analysts being employed and the targets they are tasked to address. As well as these changes, intelligence projects and missions have become more complex. Moreover, the increased activities associated with post-9/11 intelligence have resulted in privatising some aspects of intelligence work. As an indicator, we are now seeing scholarly texts appear in the subject literature that are specifically addressing the privatisation of intelligence as a topic—one such book is reviewed in this special issue of *Salus Journal*. The topic of privatisation of intelligence was discussed in its worldwide context during a one-day symposium in Canberra on 8 August 2013.

The symposium was hosted by Charles Sturt University and the Australian Research Council Centre of Excellence in Policing and Security, and was held at the National Press Club. Dr Troy Whitford, a lecturer in history and politics at Charles Sturt University, was the symposium's convenor. During Dr Whitford's opening address to the delegates, he pointed out that intelligence activities such as agent and analyst recruitment, open-source information gathering, covert surveillance, and data analysis are being privatised. In response, private investigation firms are now contracting services to government and non-government organisations, as well as the corporate sector.

* Corresponding author: twhitford@csu.edu.au

Dr Whitford welcomed speakers at *The Privatisation of Intelligence* symposium who included: former Australian Federal Police Commissioner Professor Mick Palmer, AO, APM; Head of the Olympic Intelligence Centre and the National Olympic Intelligence Project for the London 2012 Olympic and Paralympics Games, Ms Sue Wilkinson; Director at Civil Liberties Australia, Mr Tim Vines; and Assistant Inspector-General of Intelligence and Security, Mr Jake Blight.

Papers presented at the symposium were considered for inclusion in this special issue of *Salus Journal*—we are pleased to be able to present two critical essays and three unclassified papers representing the sampling of perspectives of the practitioners and academics who attended. We commend these papers to you as examples of "the private world of intelligence," and in doing so extend our gratitude to the Editorial Board's Associate Editors for giving of their time to review them.

- o O o -

Critical Essay

BENEFITS, CHALLENGES, AND PITFALLS OF PRIVATE INTELLIGENCE

Mick Palmer, AO, APM†

It was my pleasure to give the opening address at the Privatisation of Intelligence Symposium hosted by Charles Sturt University and the Australian Research Council Centre of Excellence in Policing and Security. In this paper I draw from that address, my policing career and my involvement in key strategic and operational reviews and inquiries on behalf of government. My focus is to discuss from a practitioner's perspective, core concepts of intelligence and information sharing in the Australian context. It is underpinned by the fact that the privatisation of intelligence is a reality and has been for some years. With this as the starting point, I go on to challenge policy concepts that do not recognise this reality and assess the benefits, challenges and pitfalls of the privatisation of intelligenceand intelligence sharing in Australia. I conclude with remarks about what this might portent for future policing and policy leaders.

Keywords: Intelligence, private investigation, need-to-know doctrine, need-to-share doctrine, right-to-know doctrine.

THE AUSTRALIAN CONTEXT

In Australian policing and public services, the extent and nature of outsourcing is a contentious yet significant policy issue. Outsourcing and privatisation are a reality premised on the limitation of government resources to meet an ever expanding public demand for services. The outsourcing or privatisation of intelligence, once considered the sole domain of policing and intelligence agencies, is an inevitable part of Australia's policing and policy future. However, it does need to be examined in light of the reluctance of governments

† Corresponding author: MPAassociates@bigpond.com

in Australia to share intelligence beyond a narrow framework. What is essential is that this narrow framework is broadened to include more complete intelligence sharing with private industry bodies including multi-national corporations who have a legitimate "right-to-know."

From the perspective of being an *inclusionist* and not an *exclusionist*, I consider that in Australia, for decades we have found a million reasons not to share intelligence when the consequences of taking the risk of doing so were far too great to overcome. While there has certainly been a loosening up of an earlier more conservative and rigid approach, Australia has been slow to shift policy gears in this area. In Australia we have tended to get caught up in the *need-to-know* versus the *need-to-share* doctrine. A rigid approach to intelligence exchanges that does not recognise the role and contributions of the private sector, leads to far too many incomplete pictures.

INQUIRES AND INTERNATIONAL PERSPECTIVES

The United Kingdom (UK) and the United States of America (USA), by contrast, have adopted an overarching policy position that is less risk averse than we have seen to date in Australia. The UK and the USA are more willing to take risks about sharing intelligence and more willing to share openly with the private sector. In making this comment, I draw on my experiences in conducting a number of national and international inquiries on behalf of the Australian government.

In many ways, a number of those inquiries have had at their core, the consequences of taking a traditional view of sharing intelligence and not stretching to find non-traditional links and channels for sharing intelligence. This has at times been driven by a fear on behalf of those holding intelligence of being accused of passing on information they should not and as a result, not passing it on at all. Intelligence tensions between government and policing agencies and the private sector also tend to be exacerbated when there is a failure to recognise that a traditional focus narrows the potential intelligence base which inevitably leads to incomplete intelligence pictures.

A key risk to completing the intelligence picture also comes from government and policing agencies failing to recognise that many of the large multi-national companies that own and operate key civil infrastructure in Australia, have very sophisticated intelligence arrangements within their companies. In reality, it is often these companies that have a far better overall

intelligence picture about security threats to their infrastructures than government agencies, including intelligence agencies. This is largely because many of these companies operate internationally in regions of serious piracy and threats of terrorism. Therefore, the collection and assessment of a broad spectrum of intelligence is undertaken within this private sphere to develop security plans and responses.

My own experience is that despite there being evidence of intelligence gaps, Australian policy has been slow to shift gears and recognise the value in mutual exchanges of intelligence based on trust. In reality, the risks we take from not sharing are far less than the consequences we always face in not doing so. We need to actively look for ways to share rather than reasons not to.

CHALLENGES, BENEFITS AND BARRIERS TO INTELLIGENCE SHARING

Having identified that there are significant risks of not sharing intelligence and in not taking a broad view of the intelligence base, it is necessary to look beyond the dominant policy position to examine the broader benefits and barriers to intelligence sharing.

There are clear and important differences between the operation of public intelligence agencies and private intelligence agencies. These differences arise not only because the former is taxpayer funded and the latter business and profit driven, but in the underlying business models and corporate priorities of the private sector that use the intelligence product. The business driven private sector makes them much more likely to be highly motivated, to focus on the security outcomes that will be achieved by the use of intelligence products and much more likely to minimise processes that impede sharing of intelligence.

The amount of intelligence that is shared in the private sector and between major multi-national companies that own and operate major civil infrastructures is substantial. In their day to day operating environments, there are clear pressures for any intelligence product to be valuable to the respective company in terms of its reputation, its profits, protection from industrial/economic espionage, and the potential to expand its business into new areas. These corporate priorities create an ongoing business demand for targeted intelligence product that is integrated into strategic and operational decision making. This business imperative does not often exist in government circles outside of responding to new and emerging threat.

A core challenge in Australia is the historical reticence to fully develop genuine two-way intelligence sharing between public intelligence agencies and the private sector. In my experiences, my assessment is that government agencies tend to engage with the private sector in terms of intelligence when there is a specific interest for them in doing so. In these instances, an agreement is reached and the private sector intelligence product is shared. Nevertheless, industry has been very vocal in its criticism of government agencies that this is not reciprocated. There are key challenges as well as significant benefits for this to be more strategically addressed in Australia.

In working through these challenges, a key factor will be raising the bar of mutual understanding. What has become clear to me is that government has a very incomplete level of understanding of the value to the overall intelligence picture that can be provided by private intelligence sources. As a result governments are reluctant to share intelligence. This is because governments do not have a sufficient understanding of what is potentially on offer and therefore how if properly utilised and managed through a genuine partnership, the benefits that can flow to both sectors.

In government we can get caught up with reasons for not sharing. The focus should be on what avenues there are for sharing intelligence. The challenge is to strike the balance between genuine security threats without diminishing the rights of people to go about their lawful business. What is essential is that parameters are set around what is to be collected, who will analyse it and what is done with it.

CONCLUDING REMARKS

In conclusion, it is my view that private intelligence is a fact of life and it will continue to have a role to play in Australia. With this in mind, what is essential is a better understanding of some of the differences, limitations and the inhibitors to a full exchange of intelligence between government and policing agencies and the private sector and private intelligence agencies. The challenge to current and future policing and policy leaders is to look for ways to share rather than reasons not to. It is through doing this that both sectors can be better assured of a more complete intelligence and therefore security picture.

ABOUT THE AUTHOR

Mick Palmer, AO, APM, is a distinguished law enforcement professional who has conducted sensitive governmental and corporate inquiries since his retirement as Commissioner of the Australian Federal Police in 2001. Palmer conducted a number of reviews and inquiries for both the Federal and State governments as a private consultant, including the high-profile 2005 *Cornelia Rau Report*. He took up the role of Federal Government Inspector of Transport Security in 2004. Between 2004 and 2012, Palmer headed many sensitive reviews and inquiries with many of his inquiry reports being tabled in Parliament. He stepped down from his position as Inspector of Transport Security in June 2012 and is now an Adjunct Professor at Griffith University, Queensland, Australia.

- o O o –

Critical Essay

The London 2012 Olympic and Paralympic Games Olympic Intelligence Centre: Lessons Learned from Working with the Olympic Sponsors and the Private Sector

Sue Wilkinson

This paper is a reflective discussion that critically describes the role of the Olympic Intelligence Centre (OIC) played in the delivery of a safe and secure London 2012 Olympic and Paralympic Games. In particular, it examines how the OIC worked with the Olympic Sponsors and the wider private sector to provide them with the classified intelligence and information they needed to play their role in the safety and security operation effectively. Issues discussed include the cultural, statutory and systemic challenges that had to be overcome; how relationships were built to allay concerns and build trust and confidence; and the process that was put into place to allow the exchange of classified intelligence that supported the Sponsors and private sector in their operation. It details how the OIC worked with Sponsors to allow them in turn to exchange intelligence they held in their systems with the OIC, thus completing the intelligence cycle, enhancing the security operation. The article concludes with an outline of the lessons learned that were deduced through a reflective process and are offered to practitioners for consideration in future intelligence work involving the private sector.

Keywords: private intelligence; security intelligence; Olympic intelligence; terrorism; counterterrorism

BACKGROUND

The Olympic Intelligence Centre (OIC) was set up as a multi-agency "all-threats all-hazards" intelligence centre in support of the delivery of a safe and secure London 2012 Olympic and Paralympic Games (the Games). Its role was to be the single organization that protected the established UK intelligence infrastructure by providing a single point of contact for the Olympic-specific

intelligence operation, and managed and responded to demands and enquiries from what was a very wide and unique Olympic customer base. The OIC was at the centre of the threat assessment and intelligence gathering operation, and produced composite all-threat intelligence reports and problem profiling that no other organisation had the capacity, capability or appetite to deliver.

Over 100 organisations contributed intelligence, knowledge and assessment to the OIC. Potential threats included domestic and international terrorism, domestic extremism, protest and public order, serious and organized crime, international tensions and cyber threats as well as natural and malicious hazards. The OIC consolidated contributions into composite reports. Reports were produced across a range of classification levels, including, towards Games-time itself, at "non-protectively marked" (NPM)—such was the range of the demand. As well as regular all-threat intelligence reports, the OIC also produced threat assessments, briefings and responses to information requests from its wide range of customers—for example, on high profile individuals, crime groups, specific events such as the Olympic Torch Relay (OTR) and the Opening and Closing Ceremonies, and the likely impact of single issues on the Games, such as particular crime types or single threats.

All OIC products were designed for multiple use: by operational commanders to plan their mitigations and shape their operations; to provide the wider Olympic and Paralympic family with an accurate assessment of the threat picture; to inform security officials from some participating nations; to brief Government Departments and Ministers, national law enforcement agencies and the security and intelligence agencies, Olympic Sponsors and the wider private sector. Hence the need for reports at varying levels of classification.

"OLYMPIC INTELLIGENCE"—WORKING DEFINITION

The definition of "Olympic Intelligence" that the OIC worked to was agreed with all partners when the OIC was established:

> Intelligence that identifies or suggests a clear or direct threat to the security or safety of the London 2012 Olympic and Paralympic Games, including competitors, organisers, officials, venues and infrastructure;
>
> and/or

> Intelligence that identifies or suggests any criminality or action that either by its nature or association with the Games causes damage to the integrity of the Games.

It was clear that the private sector, and particularly the 55 Olympic Sponsors, would be affected by any number or combination of the identified threats. As the Games approached, it also became increasingly clear that the demand from them for a proper understanding of their own operating environment within the context of the Games would have a greater impact on the OIC and its contributors than had been originally anticipated.

THE OLYMPIC SPONSORS

There were 55 Olympic Sponsors altogether, providing a wide variety of support to Games delivery (These sponsors are listed in the Appendix). They ranged from large multi-nationals, to major British companies, to smaller enterprises, both British and foreign. They had varying expectations of the OIC, and some were far more interested in working closely and collaboratively than others. The OIC adapted its services accordingly.

Clearly, existing threats to some Olympic Sponsors could have implications for them and the Games, both in terms of general security and their corporate reputation. It was critically important to build a trusted relationship with Sponsors in order to be able to brief them in a secure environment, so that they in turn felt comfortable to share intelligence and information about their own vulnerabilities that would not normally be in the public domain, or even automatically shared with the police. Any inappropriate or inaccurate mishandling of private sector information or intelligence might have led to issues for commercial confidentiality, corporate reputation and brand name, and media issues which could, for example, even have affected share prices.

Many of the Olympic Sponsors (and other private sector partners) had excellent intelligence facilities of their own. There is no routine established, systematic and trusted common exchange of intelligence and information between the private sector and law enforcement in the UK, although many good and productive relationships and partnerships have always existed between different sets of partners for specific purposes.

With hindsight, the OIC was surprised at first when it became clear that many companies did not readily trust the OIC with their data and information,

and were very unwilling to share it, despite all the facilities and expertise the OIC had in place to ensure that their sensitive information was handled appropriately and confidentially. A great deal of collaborative work, planning and relationship building was needed to get to the point where the Sponsors were confident enough to entrust the OIC with appropriate intelligence.

From the OIC perspective, having access to the commercial intelligence and information on threats held by the Sponsors was essential to completing the all-threats intelligence picture. For example, companies were aware of their own protest issues, cyber vulnerabilities, serious and organized crime issues, insider threats—and had a good understanding of the impact of issues such as these on their operations. By extension, all of these threats might have security implications for the Games. Given how closely the safety and security program and the Sponsors had to work together on Games delivery, a mutual understanding of threats and intelligence relating to them was essential, to inform planning and decision making on keeping the Games safe—in terms of physical delivery, but also the integrity and reputation of all those involved (as per the definition of *Olympic Intelligence* above).

THE WIDER PRIVATE SECTOR

Staging an Olympic and Paralympic Games is an enterprise on an unprecedented scale. It involves massive engagement from across the private sector, large enterprises and small, just to keep multiple host cities and regions moving, serviced, supplied. Many of the issues described above in relation to Olympic Sponsors have a much wider application across national and local infrastructure. Sponsors were able to use their status to request Olympic-specific threat and intelligence briefings – but as the Games drew nearer it was clear that a range of other private sector providers across multiple sectors (utilities, transport, hotels, IT providers, the night-time economy as just a few examples) would not just want, but also need, informative briefings in order to operate and effectively fulfill their role in delivering a safe and secure Games.

THE OIC LIAISON TEAM

Formal engagement with Olympic Sponsors (and later the private sector) began in November 2011 after a dedicated Sponsors liaison officer was appointed to co-ordinate a small team. The OIC compiled profiles of all 55 Olympic Sponsors, and worked with other existing intelligence units, such as the National Domestic Extremism Unit, the Police Central e-Crime Unit, counter terrorism

units, and international liaison units, to assess the main threats to Sponsors. Successful ongoing engagement with the Sponsors, at regular briefings and also individual meetings, was critical to building their trust and confidence in the OIC, so that they in turn felt confident enough to share their own intelligence on threats—which in turn would lead to a more informed and effective security operation. Sponsors varied in their response but on the whole, OIC intelligence briefings were substantively enriched. The process of engagement continued right up to and throughout the Games thus ensuring that Sponsor profiles were kept up to date, and operational commanders were able to plan their safety and security mitigations accordingly.

THE KEY ISSUES AND DEBATES ON SHARING INTELLIGENCE WITH SPONSORS AND THE PRIVATE SECTOR

There was lengthy ongoing debate between the OIC and UK law enforcement, the security and intelligence agencies and with UK Government about what the nature and content of such briefings might be. At first the plan was that any briefings should be unclassified or "non-protectively marked." Given the UK's existing legislation, policy and practice in relation to classification and handling of such material, and the technical and intellectual question about whether there can be such a thing as an "unclassified" intelligence briefing, there was much discussion about whether the likely content of any such briefing was meaningful or of any practical use (The UK Government Protective Marking Scheme is included in the HMG Security Policy Framework and can be found at www.gov.uk). After much consideration by senior policy makers and practitioners, it was agreed such briefings could be compiled at RESTRICTED—subject to a suitably secure delivery method being devised.

Furthermore, some of the Sponsors (and some private sector partners) were international companies, which again affected what could be shared—some companies active in the Olympic sphere were from countries that did not have any form of established relationship or arrangements with the UK on sharing intelligence. The OIC had to be extremely careful of sharing information on Olympic threats and intelligence with foreign companies who might then, by default, be briefed on issues that their own governments were not. This was a political and diplomatic issue that again, was never fully resolved. The special nature of the Games allowed it to happen for the purposes of this event only.

The fact remains that the UK intelligence community does not widely share classified intelligence with the private sector on a routine basis. There are many systemic, structural and legal barriers to doing so. The challenge for the OIC was to develop trust and confidence enough, and to put in place a bespoke process to respond to the needs of this particular event. The reality of the statutory issues covering security, handling and accountability of both providers and recipients were met as far as they could be—training and awareness, handling restrictions and security clearances were put in place. Legal advice was sought but was not particularly conclusive. Had there been a leak or a security breach lessons would have been learned from the consequences—in the event, this was not tested.

Sponsors and private sector partners remained concerned throughout that any leaks or breaches might have a negative commercial or reputational impact on them. Their feedback to the OIC indicates that these fears were largely allayed by the processes that were put in place and the trusted relationships that were built up. The OIC, however, remained acutely aware throughout that private sector information and intelligence is commercially sensitive, and ensured it was treated with the same care and respect as any other crime or terrorism-related intelligence.

OIC intelligence reports could not be circulated by hand—a paper trail was assessed as too risky, even under established controlled handling conditions. Oral briefing of 55 Sponsors and others in a secure environment would have been logistically difficult to organize and time consuming, and briefing content would have been vulnerable to misinterpretation and onward cumulative inaccuracies. An IT solution put in place in partnership with the Centre for the Protection of National Infrastructure (CPNI) and described below, was assessed as the only viable option for sharing classified intelligence with Sponsors and the private sector (although paper circulation continued within established intelligence circles continued at RESTRICTED and at SECRET).

These arrangements were put into place incrementally, and regularly discussed at senior policy and program level throughout 2011 and into 2012, particularly as the program became more operational and entered the delivery phase from May 2012. The Olympic and Paralympic Games are such a global high profile and critically important event, a measure of pragmatism came into play—the very nature of the event allows for "special" arrangements to be made and agreed to meet the challenge. This is one of the huge opportunities offered

by hosting an event of this scale—to work differently, where doing so is the best way to meet the challenge.

THE OLYMPIC TORCH RELAY

The Olympic Torch Relay provides an excellent case study of law enforcement working closely with the private sector—in this case the three Olympic Sponsors of the Torch Relay, known as "The Presenting Partners"—Coca Cola (US), Samsung (South Korea) and LloydsTSB (now Lloyds Bank—UK).

For 70 days the Olympic Torch Relay crossed the UK, passing through high crime areas, inner cities, Northern Ireland and regions affected by a variety of local, national and international issues. Each of the Sponsors had pre-existing ongoing threats to them, particularly in the form of disruptive (as opposed to peaceful) protest. The Torch Relay was very high profile, and assessed as likely to attract attention from disruptive protestors, for example, whether protesting about their own causes and using the Torch Relay as a useful media backdrop, or protesting about the Sponsors, or against the staging of the Games. There were concerns about crime; and the period the Torch Relay passed through Northern Ireland was potentially challenging.

The Presenting Partners travelled ahead of the main body of the Relay in a convoy, engaging the crowds, handing out gifts, setting the scene. Clearly, they were potentially vulnerable, and had a strong argument for fuller intelligence briefings on a daily basis so they better understood the operating environment—to safeguard their own people, their convoy operation, and allow them to take account of upcoming issues such as expected protests in their own planning.

The business case for fuller briefing of the Presenting Partners was compelling, and it was agreed at senior policy level that given the unique circumstances of the Torch Relay RESTRICTED briefings would be made available to them. This broke new ground—intelligence was to be shared with international private sector partners, not in response to a single event or crisis where sharing intelligence might have been conducted as an exception, but on an ongoing basis as part of an extended operation. A process was put in place to provide a secure vehicle for physically getting the intelligence reports to the Presenting Partners.

THE INTELLIGENCE EXCHANGE IN PRACTICE

CPNI protects national security by providing protective security advice to public and private sector companies and organisations. Their advice covers physical security, personnel security and cyber security/information assurance on cyber and other threats, espionage and terrorism.

It was decided that CPNI would provide secure and bespoke access to OIC intelligence reports via its website, allowing accredited individuals to gain access to the reports through secure portals on the site. They would then be able to read a range of material, with access and content tailored to them and/or their organization, but they were not able to copy, alter, print or further disseminate the material—it was essentially provided on a "read-only" basis.

The CPNI solution was initially designed for the Presenting Partners on the Torch Relay; however, it was later decided to also invite all the Sponsors to apply to receive the briefings. All the Presenting Partners accepted, but not all Sponsors took up the offer. Those that did were asked to nominate an individual who would be the point of contact, and who would have to undergo a level of security clearance prior to being allowed access to the relevant secure portal. This might have been challenging to achieve, given the international organisations involved, but most companies locally employed security managers who were UK citizens so security checks were more straightforward to complete. Some Sponsors were in any case familiar with the CPNI website and used to working with it and with CPNI itself, so access approval was simpler. Nominated individuals initially completed an online security form and CPNI carried out further checks. They then attended OIC and CPNI briefings where they were provided with technical instructions and guidance for accessing the website, and an understanding of their role and responsibility in handling classified material.

Once nominated individuals had accessed the intelligence reports, it was their responsibility to forward brief on the contents within their own domain, to brief proportionately and appropriately, and take their own decisions on how best to achieve this. This was the assessed risk the OIC and CPNI took in achieving this outcome, and was covered in their induction process.

Once the decision had been taken to brief the Presenting Partners and then the Sponsors through CPNI, and it was clear that providers and recipients had confidence in the process, it was further agreed that some private sector

infrastructure providers who were already part of CPNI "business as usual" arrangements, would also have access to the OIC reports at CPNI's discretion. The same terms and conditions applied. By the time the Games were underway, the Presenting Partners, up to half the Sponsors, and a range of private sector organisations were in receipt of tailored classified (UK RESTRICTED) intelligence reports on Olympic threats. Customers of this service also had access as deemed appropriate to other reports such as event profiles—for example, the Opening and Closing ceremonies. At least some of the reports they were in receipt of contained intelligence and information they themselves had provided, thus completing a virtuous circle.

In addition, at Games time daily oral briefings for international security officials were hosted by the Olympic International Liaison Unit. An update on the day's events and likely issues were included on the agenda, and police commanders and other Olympic officials presented as needed—subjects covered might cover crime or likely protest, but also other issues such as transport, weather, or media. The police commanders used OIC RESTRICTED reports on which to base their briefings and were allowed to use their discretion on what was included and within what context—another example of fast-moving operational necessity over-riding normal precautions. It was decided that the Sponsors should also be invited to attend this briefing. OIC representatives were always present to take questions and deal with queries or concerns offline.

The OIC also produced unclassified briefings (non-protectively marked) that were forwarded to the Cross-sector Safety and Security Communications partnership, an initiative between the London Police Services, the Home Office, London First (a business networking organization) and 25 business sector groups. The partnership has created a communications structure via a telephone hub that enables members to be briefed on any relevant safety and security activity and how it might affect them. By the time briefings are disseminated many hundreds of people may have access to them, and the telephone hub is not secure. Therefore, briefings could only be unclassified. However, for the period of the Games, it was agreed that the OIC would produce a NPM briefing for inclusion at the daily telephone hub. This proved successful, but it is worth noting two things—first, that a meaningful briefing at NPM was far harder to achieve than was initially anticipated, and secondly, OIC staff were intelligence professionals and not accustomed to working in an unclassified environment, and extra training and familiarisation was required.

Feedback to the OIC and CPNI from the Sponsors and the private sector on this unprecedented range of engagement and briefing was, perhaps not surprisingly, overwhelmingly positive. The process allowed the private sector to better understand the environment within which the safety and security operation was being delivered, and allowed them to tailor their own operations and activities accordingly. With hindsight, the process should have been put in place earlier, and the intelligence cycle would then have been of a better quality earlier on in the planning phases in the years leading up to the Games. Nevertheless, there were also extensive lengthy discussions that took place at a senior governmental level, with the participating law enforcement and security and intelligence contributors, and with the Olympic delivery program, to achieve agreement to proceed—these arrangements were unique and innovative, and departed from normal practice.

LESSONS LEARNED

At the conclusion of the London 2012 Olympic and Paralympic Games in September 2012, an extensive de-brief process was undertaken on the entire intelligence operation, including with the Sponsors, and with partners of the OIC, as well as with the operational leadership group that ran the safety and security operation on a daily basis. Some clear principles emerged.

Because of the cross-sector, national and international nature of the Games, composite all-threat intelligence assessments and reports went to a far wider audience than is the norm under "business as usual." There were no security breaches that came to the attention of the OIC; no inappropriate sharing of information or intelligence was identified. All evidence indicated that the nominated individuals in receipt of the classified reports fully respected the terms and conditions and behaved entirely responsibly with the material made available to them.

The intelligence shared with the Sponsors and the private sector was at RESTRICTED only. That is not to say that had an emergency or critical incident occurred, one to one briefing at SECRET might have taken place as appropriate, as would also occur under "business as usual." But in order to achieve routine briefing at RESTRICTED, it was necessary for the contributing agencies and sources to provide their intelligence reports and assessments to the OIC at a lower classification than they normally operated at. In a fast moving, ongoing and dynamic environment such as the Olympics, SECRET reporting needs to be

at a minimum, as handling regulations then restrict access and circulation and, as operational commanders so often complain, intelligence in that format usually cannot be readily acted upon.

Therefore, the bulk of OIC material was made available at RESTRICTED—something that had not been originally anticipated. It became clear that in many cases an intelligence report at RESTRICTED did not necessarily differ hugely in content from the same report at SECRET. RESTRICTED intelligence reports could be more widely circulated, acted upon as necessary, and contained a version of the intelligence that might not have been circulated at all at SECRET. This posed the question of whether the UK intelligence community might routinely over-classify intelligence, thus inadvertently preventing wider circulation of safety and security information.

OIC intelligence reporting was routinely published in a composite all-threats format. All recipients, including the private sector, welcomed the ease of reference this provided. They also welcomed the fact that they could see threats together, allowing them to prioritise and assess the urgency of each in relation to another, thus assisting their decision making in terms of both response and allocation of resources. Normally, intelligence reports tend to be circulated by individual agencies on their area of reference only—for example, cyber, terrorism, serious and organized crime. By receiving all-threats reports they reported being able to read the reports more quickly, absorb the "whole picture" better, make prioritized decisions and manage their resources more effectively. If they wanted or needed greater detail this was provided on request to the OIC. Many of the Sponsors and private sector partners, unused to receiving intelligence reports at all, found the format and presentation of the reports user friendly from the start.

Composite all-threat intelligence reporting focused on an event the scale of the Games led, inevitably, to improved profiling - for example, of cyber threats and trends, protest profiling, links across the different threat areas that had not been identified in the same way before. It also highlighted intelligence gaps that the OIC addressed—for example, given the international nature of the Games, the OIC added the international protest picture to the national one to complete the analysis of likely disruptive activity in the UK over the summer of 2012. The contribution of the Sponsors and the wider private sector to the quality of composite all-threat reporting was significant, and endorses the value of the partnership with the Sponsors and the private sector that had been put in place.

CONCLUSION

There are many ongoing existing arrangements for engagement and information exchange with the private sector in the UK. CPNI have been cited in this paper. Police forces and law enforcement agencies routinely work closely with the private sector on prevention and detection of a wide variety of crime types—cyber, fraud, serious and organised crime, domestic extremism, terrorism to name but a few. In the event of critical incidents the normal classification rules can be lawfully put aside in the interests of an investigation and public safety. London First and the CSSC are but two examples of organisations that provide extensive networking opportunities and information exchange regularly, at an unclassified level.

The Games provided a unique opportunity to do things differently, to try out new ways of working within and across law enforcement, security and intelligence agencies, to test and adapt existing systems and processes. The integral role of the private sector in delivering a safe and secure Olympics demanded new arrangements. Over the recent past the private sector has increased its investment in intelligence, building impressive intelligence departments of their own, with a professionalised staff. The new arrangements developed to deliver the intelligence function in support of the Games delivered an enhanced intelligence picture for the benefit of all—as evidenced by the feedback from the private sector and law enforcement alike.

The *post*-Games challenge is to further test and assess the special arrangements that were put into place and extract critical learning and best practice, where appropriate building it in to "business as usual" systems and processes rather than allow it to remain particular to the Games period—and potentially forgotten.

DISCLAIMER

The critical commentary provided in this essay is by necessity nonspecific. This is because of the nature of the work it describes. As such, it has not been possible to cite specific examples of what was achieved. However, it is hoped the principles outlined here can be used when considering intelligence arrangements in the future—whether in support of a specific event, or for general application.

APPENDIX: LONDON 2012 OLYMPIC SPONSORS

1. Worldwide Partners—Coca-Cola; McDonalds; GE; Dow; Panasonic; Acer; Atos; Omega; Visa; P&G; and Samsung.
2. Official Partners: Tier One—Adidas; BMW; BP; British Airways; BT; EDF; LloydsTSB; and Procter & Gamble.
3. Official Partners: Tier Two—Adecco; ArcelorMittal; Cadbury; Cisco; Deloitte; Thomas Cook; and UPS.
4. Official Partners: Tier Three—Aggreko; Airwave; Atkins; The Boston Consulting Group; CBS Outdoor; Crystal CG; Eurostar; Freshfields Brickhaus Deringer LLP; G4S; GlaxoSmith-Kline; Gymnova; Heineken UK; Holiday Inn; John Lewis; McCann Worldgroup; Mondo; Nature Valley Granola Bars; Next; The Nielssen Company; Populous; Rapiscan Systems; Rio Tinto; Technogym; Thames Water; Ticketmaster; Trebor; Kathmandu Bazar Plaza; and Banjara Group

ABOUT THE AUTHOR

Sue Wilkinson holds a BA(Hons) degrees and was awarded the Queen's Police Medal. She joined the Metropolitan Police Service (MPS) in 1980, and held a variety of uniform, detective, policy, and strategy roles across London and at New Scotland Yard. She served in a variety of roles within the Specialist Crime Directorate before leaving for Australia in 2007 to take up a three year contract as the inaugural CEO of the Australia New Zealand Policing Advisory Agency (ANZPAA). When she returned to the Metropolitan Police Service in September 2010, Ms Wilkinson took on two roles—Head of Profession for Intelligence for the MPS, and Head of the Olympic Intelligence Centre and the National Olympic Intelligence Project for the London 2012 Olympic and Paralympics Games. In September 2011 Ms Wilkinson moved over to her Olympics role full-time. She has recently retired from the MPS following the success of the Olympics.

- o O o -

Research Article

PUBLIC AND PRIVATE INTELLIGENCE: HISTORICAL AND CONTEMPORARY PERSPECTIVES

Ruth Delaforce[‡]

Intelligence is often regarded as information that is special or different, which must be safely kept. When sought, collected or used by the private sector, as opposed to public agencies, concerns are raised on the purpose and propriety of such an activity. However, in an historical context, intelligence collection or sharing between public and private interests for the purpose of national security was not unusual, particularly during the Cold War. Case studies from this era indicate that overlapping concerns were economic success combined with political strategy. Glimpses of these shared interests between the state and business can also be identified in the immediate post-Cold War era, and the aftermath of terrorist attacks in 2001. Perhaps the greatest contemporary change is not that "private" and "public "intelligence is shared between business and state, but the extent of such an enterprise. Further issues related to this change are: state dominance in the public-private relationship; potential fragmentation in the intelligence process; gaps in the historical record; and implications for future generations of intelligence professionals.

Keywords: Intelligence; public sector intelligence; private sector intelligence, national security intelligence

INTRODUCTION

Intelligence exchange between the public and private sectors for national security purposes—particularly in relation to strategic military, political and economic issues—is not new. Global security frameworks have long been dependent on intelligence exchange between a variety of actors, state and non-state. Glimpses of such praxis can be identified across the decades since 1945, during the Cold War and post-Cold War eras, through to the "durable disorder"

[‡] Corresponding author: r.delaforce@griffith.edu.au

that characterises today's global security climate (Cerny, 1998). Most notable, however, is the paradoxical nature of intelligence exchange now occurring, with overt collection in the public domain, while data analysis by state and private actors often appears to lack transparency and democratic oversight (Chesterman, 2008, 2006; Michaels, 2008).

During the Cold War, intelligence collection reflected an "institutionalised modern state" characterised by "covert action, high politics (and) intense secrecy" (Deibert, 2003: 175; Troy, 1991: 436). In the post-Cold War era, definitions of intelligence were widely debated, where scholars sought to reframe its meaning in terms of the "market state," introducing concepts of economic, business or competitive intelligence, and noting the benefits for both the state and for-profit companies by "sharing wares" (Treverton, 2003: 69–76). Since the events of 11 September, 2001, the concept of private intelligence has broadened to include data that is specifically collected and utilised by business for its own purposes, in addition to those companies contracted by governments to perform information gathering and processing activities.

Often the importance, priority and sensitivity attached to *intelligence* is not necessarily its content, but the source of such information—where and how it was obtained (that is, through human, signals or electronic means)—or contextual contribution, adding value to what is already known (Warner, 2007: 17–27). Intelligence collected by government agencies (the public sector) raises community and civil libertarian concerns on the purpose and propriety of such acts (Miller, 2007; Wong, 2006). However, these concerns are often voiced more strongly when the private sector is involved, as has been noted recently in the case of Edward Snowden (Ball, 22 August 2013).

In an historical and contemporary context, public-private intelligence exchange has underpinned both national and international security strategies, particularly for Great Britain and the United States. This paper proceeds with a summary of such strategies and case studies, during the Cold War, the post-Cold War era, and since 2001, where intelligence has gained precedence. The case studies illustrate British and American approaches towards public-private intelligence gathering and exchange. For the United States particularly, such public-private exchange has raised significant legal issues relating to privacy and lack of transparency. While the cases in this paper are demonstrative of these issues, there is limited scope to review in-depth the differing trans-Atlantic legal

regimes; the focus instead will be the changing concepts and state acquisition of intelligence that has occurred since 1945, and emerging issues.

Aside from the September 11 initiator of religious extremists prepared to use violence, intelligence is now aligned to other societal shifts, of globalisation, the growth of technology, and securitization across a range of government policies and programs. Tracing these changes in intelligence concepts since 1945, it is possible to identify the trajectory towards public-private partnerships, where "intelligence is now big business" (Herman 1996: xii).

In noting this intelligence sharing, four problematiques—emerging or potential problems—are reviewed. The first problematique considers the public-private relationship and state dominance of intelligence exchange. Secondly, the fragmentation of an intelligence process which, for those involved in national security analysis, can pose issues of information overload. Thirdly, the potential consequences from gaps in the historical record, related to archival limitations on privately collected intelligence. The last problematique posits the future loss of distinction between public-private sector employment for aspiring intelligence professionals.

THE COLD WAR

For intelligence professionals, the years between 1946 and 1989 have been described as a linear framework that was reasonably predictable (Liaropoulos, 2006: 6). In this era, public-private partnerships in both Great Britain and the United States (US) may be construed as a mutual patriotic opposition to communism. Intelligence during this era was derived from both human and electronic sources, was rigorously censored, and focused upon "strategic military arrangements" and countering the nuclear threat (Steele, 2002: v). Alternatively, private sector activities could also be considered illusory, with "front companies" that comprised personnel either recently retired or seconded from public security agencies.

One of the first glimpses of a public-private partnership in intelligence exchange is that of the International Diamond Security Organisation (IDSO), created in 1954 by Sir Percy Sillitoe (Sillitoe, 1955). Prior to retirement and founding of this company, Sillitoe was a former Chief Constable of Police, then head of MI5, the British internal security service. Soon after retirement, Sillitoe was approached by representatives of South African company, De Beers, a major diamond producer and exporter.

De Beers had concerns with diamond smuggling operations across the African continent that were undermining their control of the market, and Sillitoe was contracted to identify and disrupt these illegal activities (Fleming, 1957). Sillitoe did so by creating "an intelligence network which would penetrate" across Africa and the world, recruiting both former and serving British security agency personnel. Travelling between South Africa, Ghana, the Belgian Congo, Tanganyika and Sierra Leone, Sillitoe received a good deal of unofficial cooperation from intelligence officers located in these colonies, reportedly facilitated by Whitehall (Epstein, 1982; Fleming, 1957). This private intelligence network was deemed to have successfully eliminated the illicit trade, with the company being wound up two years later.

Established to support the market operations of a major diamond producer, IDSO was involved in the collection of private intelligence for private sector advantage. However, the involvement of public police and state security agencies is curious. One explanation is that, at the time, there were concerns by Western states on the Soviet expansion of its heavy industry manufacture, notably the production of military hardware (Epstein, 1982: 'Chapter 17'). Integral to these production processes were industrial diamonds (Dumett, 1985: 385–386). Therefore, reducing a flow of black market diamonds could impede Soviet industrial expansion. Intelligence exchange in the IDSO case occurred across the public-private sector, and collaboration would appear to be for two divergent purposes, politico-military strategy, and maintenance of a private monopoly. Also integral to this process were the use of sensitive sources and methods, represented by the cooperation of colonial intelligence officers, and employment of mercenaries to intercept diamond smugglers (Fleming, 1957; Kamil, 1979).

A further glimpse of public-private intelligence exchange may be ascertained from the North Yemen civil war of 1962 to 1970. The civil war commenced when the incumbent Imam al-Badr was deposed by a military junta, supported by the Soviet Union and Egypt (Curtis, 2004: 288–303; Fattah, 2010: 31–32). An insurgency by the ousted Royalists to regain power was supported by a British private security company led by Sir David Stirling (Connor, 1998: 192–195; Curtis, 2004: 295–303; Dorril, 2000: 684–686). Stirling, formerly founder of the British Special Air Services (SAS), recruited other SAS veterans through a private company, Television International Enterprises (TIE) based in London.

While the TIE self-identified as a private security company, many of its operations—surveillance, communications and targeted assassinations—were alleged to have assisted Western intelligence. In one instance, by identifying the use of Chinese-manufactured poison gas released from Egyptian aircraft; reports indicated that a British contractor was blinded and other Royalist tribesmen died from exposure (Kemp cited in Connor 1998: 194; Geraghty, 1981: 117). Although intelligence was purportedly derived from a private source, the preponderance of "former SAS men, and officers and troopers who were still serving with the Regiment" while working for Stirling, suggests at least some government facilitation (Connor 1998: 194).

Not all public-private intelligence exchange centred upon mercenary actors. Hulnick (1996: 18) notes instances of public intelligence supporting private US and British interests, particularly companies located in countries where incoming Marxist governments threatened to nationalise industry. In these cases, Western intelligence agencies supported covert activities and coups to remove such governments. During the 1950s, former government security personnel were employed by British Petroleum (BP) operations in Iran as security specialists. The company was included on distribution lists for British-derived intelligence, at a time when Mohammad Mossadegh, an Iranian leader, was threatening to nationalise foreign business operations (Prados 2006: 99; Smith 1982: 119–120).

This private intelligence net ceased in August 1951; Mossadegh was later ousted with the assistance of both US and British security services (Prados 2006: 99; Risen, 2000; Smith 1982: 119–120). Further examples include a 1954 US-sponsored coup instigated in Guatemala, following threatened nationalisation of the US-owned United Fruit Company; and Chile in 1970, with concerns raised by the American owned International Telephone and Telegraph Company, said to have influenced a US-sponsored removal of the Allende Government (Schlesinger & Kinzer, 1999; US Committee on Foreign Relations, 1973).

THE POST-COLD WAR ERA

Instances of public-private intelligence exchange can also be identified in the post-Cold War era. Between 1990 and 2001, the concept of intelligence changed, threats from nuclear-armed political adversaries were lessened, while potential benefits for the commercial sector and economic superiority were being promoted (Krizan, 1999; Herring, 1999 Shelley, 1995). Key factors at this time

were the reduction in military and security personnel employed by government agencies, increasing privatisation (particularly in the control and deployment of technological assets such as satellites) and realisation by industry that the state could not always guarantee protection (Berkowitz, 1996; Unsinger, 1999). The global security picture had changed, with a multiplicity of threats emanating from state and non-state actors, comprising criminal, religious, nationalist and ideological groups. Emphasis was also placed upon the market state, described as an economic battlefield (Wright, 1991: 209). Krizan (1999: 8) notes that, rather than intelligence being a government to government exchange, the environment was "receptive to government-private sector interaction."

The use of public intelligence to support private commerce was identified by CIA Director, Robert Gates, as necessary where "governments … try to steal our technology unfairly or illegally to disadvantage American business" (cited in Hulnick: 461). During the 1990s, Todd and Bloch (2003: 55) note that US government provision of intelligence to the private sector meant that American companies "won US$145 billion of business after government intelligence operations identified and defeated bribery or unfair conduct by foreign competitors." France also reportedly employed public intelligence resources to benefit French business (Hulnick, 1991: 459). Of particular concern was in-house intelligence collection by Japanese mega-corporations, such as Mitsubishi in New York, while other companies were beneficiaries of "overtly and covertly obtained economic and technical intelligence by the Japanese Ministry of International Trade and Industry" (Madsen, 1999: 436–437).

A notable feature of this era is the provision of training by former government security personnel to the private sector. Herring (1999) refers to the benefits for the private sector through adopting government approaches to intelligence, identifying priorities, processes and competitors.

Steele (1998) advocated an alternative option, that the private sector could support government agencies through more efficient provision of specific services such as commercial imagery, foreign language assistance, market research and media monitoring, all categorised as open source intelligence. Privately acquired data collections were also recognised for their potential assistance to business and academia. Examples include the creation of an intelligence network and investigation services for the maritime industry, the acquisition and maintenance of a private intelligence database on terrorism by an

academic institution, and the development of a global competitive intelligence organisation (Dugan, LaFree & Fogg, 2006; Unsinger, 1999).

Public-private intelligence exchange was also crucial in counterinsurgency operations, particularly for emerging private military and security contracting companies (Shearer, 1998; Silverstein, 1997). In one case, the private military company, Sandline—contracted by the Papua New Guinea government in 1997 to undertake a counterinsurgency operation and recapture the Panguna copper mine in Bougainville—was allegedly supported through the provision of signals intelligence by Great Britain and the US (Madsen 1999: 248–249; Todd & Bloch, 2003: 112). Sandline reportedly also had access to an in-house company—Quantum Strategic Consulting—that specialised in intelligence collection and analysis (Brooks, 1999).

Unprecedented growth of the internet during this timeframe was noted by one observer as potentially "the most fabulous surveillance program ever invented" (Young, cited in Todd & Bloch, 2003: 35). The internet also facilitated the collection of open source intelligence leading to private sector involvement in the process (Steele, 1995). Madsen (1999) charts the growth of the internet from its origins as a Cold War defence project, to its capacity for both public and private cyber-intelligence collection.

The transition of many defence-initiated projects from military control to the private sector occurred during this era, with 120 private companies being involved in the launch of more than 1,000 satellites, in turn, facilitating open access to technologies such as Global Positioning Systems (GPS), satellite telephones and detailed maps (Brooks, 1999; Todd & Bloch, 2003: 35–70). It is in the post-September 11 era, however, that intelligence exchange has undergone a transition; data, technology and personnel now increasingly operate across the public-private domain.

THE GLOBAL WAR ON TERROR

The declaration in 2001 of a global war on terror by US President, George W Bush (2001) signalled a change to the public-private intelligence relationship. While threats emanated from state adversaries and religious extremist groups, the assessments were also including individuals labelled as *lone wolves* and criminal networks. Further, the concept of security was applied to diverse programs related to food, water, natural resources and health (Buzan, Waever and De Wilde, 1998). The so-called "information revolution" that began in the 1990s

challenged the capacity of state intelligence agencies. Liriapoulos (2006: 8) notes these vulnerabilities as resulting from a lack of resources, loss of state monopoly and inability to restrain technological development—which can be utilised by anyone—in addition to significant reliance by the state upon commercial information infrastructure.

The reduction of state-employed intelligence personnel during the 1990s resulted in a critical manpower shortage for the counterterrorism campaigns after 2001 (Voelz, 2006: 12–13). The battlefield required personnel who could manage "the explosion in multilingual digital information," in addition to the more traditional ground-truthing expeditions (Steele, 2002: v–vi). Government responses have been to contract private sector personnel—foreign linguists and translators, military and security officers, interrogators and intelligence analysts—to augment state resources (Voelz, 2006: 12–21).

In the decade since 2001, private sector intelligence contracts are estimated to cost the US government between US$42 and 45 million annually (Chesterman, 2006: 1,058; Shorrock, 2008). The proliferation of private companies and personnel involved in intelligence activities is estimated to be 1,271 government organisations and 1,931 private companies, across 10,000 locations in the US, and comprising 854,000 personnel (military, civilian and contractors) with top secret security clearances (Priest & Arkin, 2010). A *Washington Post* investigation further estimated that this public-private endeavour produced 50,000 intelligence assessments annually (Priest & Arkin, 2010). Privatisation is also occurring in other countries, with the British General Communications Headquarters being subject to partial private sector contract management of its infrastructure, data streams and staffing (Aldrich, 2009: 899). While the state contracts private intelligence companies and their personnel, it also acquires data initially collected by the private sector.

Increasingly, citizens interface with the private sector, not government agencies; this interface and privately-derived intelligence occurs across the commercial, financial and telecommunication sectors (Michaels, 2008: 908). Either reluctantly or willingly, data held by the private sector is being provided to state agencies, where it is then often processed by private contractors (Chesterman, 2008). With an estimated 6 billion mobile telephone users and Internet access for 2.4 billion people, the capacity for governments alone to collect and process data is unaffordable and unachievable, particularly when this

data is held by the private sector (Internet World Stats, 2012; Steele, 2002: 21; World Bank, 2012).

Software and telecommunication companies, such as Google, Apple and Verizon, are of specific interest to government, with allegations that, in the US, intelligence analysts may sift through electronic data with no prior authorisation (Greenwald, 2013). In this regard, Chesterman (2008: 1,059–1,061) notes that, despite the existence of legislation requiring judicial oversight for state access to privately-sourced data, the secret cyber-collection programmes run by the National Security Agency may well preclude any requirement for a warrant. In this context, the hosting of social media sites (such as *Facebook*, *YouTube*, and *Instagram*) through telecommunication and software providers also can facilitate the (secret) gleaning of personal data (often self-disclosed by users) for state agencies (Gellman & Soltani, 31 October 2013; Kaplan & Haenlein, 2010). The collection of this personal data for targeted advertising by companies such as *Google* has resulted in multi-million dollar fines for privacy breaches (The Australian, 2012). As Michaels (2008: 902) notes, private organisations have the capacity to collect information "more easily, under fewer legal restrictions than governments."

Public-private intelligence exchange is also occurring on the territorial battlefield. In 2007, a private military company (Aegis) based in Iraq was collecting intelligence on infrastructure and convoy security threats, militia groups and criminal gangs, producing detailed maps, establishing an operations centre to collate and analyse data (Fainaru & Klein, 2007). In further examples, the private military contracting sector also offers services that include interpreters, linguists, and "human intelligence collectors" (Aldrich, 2009: 899; Voelz, 2006: 18).

Since 2001, public-private intelligence exchange appears to be mutually beneficial, with significant financial profits to companies directly contracted to undertake collection and analysis by the state. But, there is less benefit in such a partnership for companies whose core activity is not intelligence processing on behalf of the state, but where data acquired during normal business practice is then deemed to be valuable public intelligence. As Michaels (2008: 926–928) notes, the private sector is not an equal partner, being vulnerable to state pressure. Similarly, intelligence gathered through private security operations in conflict zones may be appropriated by the state. One critic of the Aegis operations centre in Iraq stated that any intelligence generated from private

contractors was "classified secret by the military and not distributed" thereby deterring wider contractor participation (Holly, cited in Fainaru & Klein, 2007).

It is unlikely that the current trajectory towards public-private intelligence exchange will cease. Instead, with the advances in digital technology, not only will the volume of data increase, but also the type of information that can be collected. This data proliferation is leading to a dispersed intelligence network, in contrast to the Cold War linear frameworks, and a need for burden-sharing through public-private partnerships (Berkowitz, 1996: 8; Steele, 2002: 21). There are a range of concerns highlighted in public-private intelligence exchange, of which four emerging or potential problems are considered in the following section.

PROBLEMATIQUES

The blurring of a public-private division on information collection, and the broadening concepts and appreciation for the utility of intelligence, are rapidly transforming the industry and its practice. This evolution is considered in the following section from four differing perspectives. These are nominated as: the unequal relationship between the public-private sectors and state dominance; fragmentation of the intelligence process and information overload; a potential for gaps in the historical record due to private sector ownership of data; and implications of public and private sector employment for future generations of intelligence professionals.

The electronic footprint of those with access to a mobile phone and the internet—estimated in 2012 to be 6 billion and 2.4 billion, respectively—occurs primarily through the private sector. A large proportion of these users are recording their lives online, with self-disclosure and dissemination that ultimately can be collected for commercial as well as security purposes. Michaels (2008) argues that the private sector has fewer legal restrictions than the government in collection and distribution of this digital data, but also notes that business is not an equal partner in the public-private relationship, being vulnerable to state pressure.

In turn, this creates an accountability gap, where business may be pressured into providing informal intelligence to the state, either due to patriotism, a misleading belief in government authority, or lack of knowledge on legal compliance (Michaels, 2008: 926–928). Similarly, government acquisition and restrictions upon privately derived intelligence also occur in military

operations, as noted in the Aegis case (Fainaru & Klein, 2007). Rather than a partnership, the inference is an ongoing "privatisation of state surveillance" across "multiple institutions" in the public-private sectors (Newkirk, 2010: 43–44).

The second problematique is a potential fragmentation in the intelligence process. The increased range of intelligence sources pose challenges for data collectors and analysts. Identifying gaps in the intelligence collection is challenging, but then knowing where such information may be sourced from is increasingly affected by the range of available sources, often referred to as information overload. Vulnerable points in the process are collection and collation of intelligence. While focus is placed upon the interchange of intelligence between and within government agencies, the number of private sector actors collecting data can also impede the process, in addition to issues of quality assurance (Liriapoulos, 2006: 15). After reviewing a US Defence Department program, a senior military officer noted that he was "Not aware of any agency with the authority, responsibility, or a process in place to coordinate all these interagency and commercial activities … The complexity of this system defies description" (Vines, cited in Priest & Arkin, 2010). A paradox of such information overload is that threats are more likely to be overlooked.

The third problematique to be considered is the (lack of) contribution to historical records. In most Western countries, government records are archived under legislation. While public access to these records may be limited, there is still a legal requirement to retain and store the data. Doing so enables historians, researchers and the public to (eventually) construct a picture of past events. Steele (2002: 20) argues that "the most fundamental, the most neglected (issues are) the lessons of history."

Nonetheless, in the contemporary era of public-private partnerships, private collectors are not bound to public rules, such that retention, storage, and later public access to records may occur. In this context, government records may identify the final outcome, but remain silent on processes of collection. For government agencies and analysts, this also introduces gaps in corporate knowledge, event chronology, and limited understanding of best (or worst) practice and available strategies. An alternative perspective is that a well-orchestrated intelligence operation should avoid identification and scrutiny (i.e. counterintelligence), and in an era of multiple threats, employing private agents may assist in this process (Prunckun, 2013).

The final problematique is a *potential* issue of concern: whether a public-private employment distinction can be maintained for future generations of intelligence professionals. During the Cold War and post-Cold War eras, it was not unusual for former state security agents to transition into private sector careers upon retirement. Miller (2007) contends there is a growing need for intelligence professionals in both the public and private sectors, while Steele (2002: 29) suggests that state employment should occur after training in the private sector. Shorrock (2008: 14) notes, however, a former CIA officer's observation, that "Everyone … is leaving and going into contracting, whether they are retiring or not," presumably enticed by the significant financial incentives. Notably, the career aspirations of younger generations such as Gen Y or Millenials do not centre on employer loyalty, but instead skills development and rapid promotion (Ng, Schweitzer & Lyons, 2010).

For future intelligence professionals, the blurring line between private-public partnerships may mean that, rather than a "revolving door," there is little distinction between work conducted for government or business, possibly leading to a blurring of patriotism and commercial ambition. Still, a third form of loyalty may be emerging, as indicated in the Edward Snowden case, and that is to the community or citizenry, rather than the state or company. Although the Snowden revelations had often been framed as whistleblowing, an underlying theme in such exposures is that of alerting citizens to the actions of their governments. A similar feature of Snowden (and other cases, such as Bradley Manning) is their age—30 and 25 years, respectively. Ng et al. (2010: 283) argue that a particular feature of this younger professional cohort is "their high expectations for social responsibility and ethical behaviour on the part of their employers."

For state intelligence agencies, however, the Snowden case may initiate a revocation of its previous policies and practices, with a reduction in private contracting and, instead, direct state employment of intelligence professionals. A further issue is that of the contractor company's role in managing its personnel, and state expectations in addressing potential leaks.

CONCLUSIONS

Public-private intelligence exchange is not a new phenomenon. As the above case studies illustrate, state and business have long had mutual interests in maintaining political and economic security. However, technological

development and open access have contributed to an exponential increase in the volume and types of raw data that may be considered of value, and therefore collected for both commercial and security purposes. It is unlikely that this trajectory will slow or cease.

A novel feature of this phenomenon, though, is that the distinction between a public-private interface is becoming less clear, with the migration of data and personnel across a permeable boundary. For intelligence personnel, the question is whether loyalty to the state is seen through the prism of both private and public sector employment. For the state, this public-private trajectory may be slowed due to concerns with security leaks from private contractors. For business, state capacity to appropriate privately-sourced data, and infiltrate and manage private operations, indicates an uneasy, if also unequal, relationship, and one which will be difficult to resist.

REFERENCES

Aldrich, Richard J. (2009). "Beyond The Vigilant State: Globalisation and Intelligence." *Review of International Studies* (35) 899–902.

Ball, James. (22 August 2013). "Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far." *The Guardian*. [http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations] last accessed 1 September 2013.

Berkowitz, Bruce D. (Summer 1996). "Information Age Intelligence." *Foreign Policy* (103).

Brooks, Douglas J. (July–September 1999). "The Business End of Military Intelligence: Private Military Companies." *Military Professional Intelligence Bulletin.* [http://huachuca-usaic.army.mil/mipb/HTML%20July-Sep99/brooks/brooks.htm] last accessed 1 September 2013.

Bush, George W. (20 September 2001). *Presidential Address to the Nation.* Washington DC. Transcript available at [http://edition.cnn.com/2001/US/09/20/gen.bush.transcript/] last accessed 1 September 2013.

Buzan, Barry, Ole Waever and Jaap De Wilde. (1998). *Security: A New Framework for Analysis*. Boulder, Co: Lynne Rienner.

Cerny, Philip G. (Spring 1998). "Neomedievalism, Civil War and the New Security Dilemma: Globalisation as Durable Disorder." *Civil Wars*. (1) 36–64.

Chesterman, S. (2008). "'We Can't Spy … If We Can't Buy!' The Privatization of Intelligence and The Limits of Outsourcing "Inherently Governmental Functions."' *The European Journal of International Law* (19:5) 1,055–1,074.

Chesterman, S. (2006). "The Spy Who Came In From The Cold War: Intelligence and International Law."*Michigan Journal of International Law* (27:4) 1,071–1,130.

Committee on Foreign Relations, United States Senate. (21 June 1971). *The International Telephone and Telegraph Company and Chile, 1970–71*. Washington DC: US Government Printing Office.

Connor, Ken. (1998). *Ghost Force: The History of the SAS.* London: Orion Books.

Curtis, Mark. (2004). *Unpeople: Britain's Secret Human Rights Abuses.* London: Vintage.

Deibert, Ronald J. (2003). "Deep Probe: The Evolution of Network Intelligence." *Intelligence and National Security.* (18:4) 175–193.

Dorril, Stephen. (2000). *MI6: Inside the Covert World of Her Majesty's Secret Service*. New York: The Free Press.

Dugan, Laura, Gary LaFree & Heather Fogg. (23–24 May 2006). "A First Look At Domestic and International Global Terrorist Events, 1970–1997." *Intelligence and Security Informatics. IEEE International Conference on Intelligence and Security Informatics.* San Diego, Ca.

Dumett, Raymond. (October 1985). "Africa's Strategic Minerals During the Second World War." *The Journal of African History* (26:4) 381–408.

Epstein, Edward Jay. (1982). *The Rise and Fall of Diamonds: The Shattering of a Brilliant Illusion.* Simon and Schuster. [http://www.edwardjayepstein.com/diamond/chap17.htm] last accessed 1 September 2013.

Fattah, Khaled. (November 2010). "A Political History of Civil-Military Relations in Yemen." *Alternative Politics* (1) 25–47.

Fleming, Ian. (1957). *The Diamond Smugglers.* London: Jonathan Cape.

Gellman, Barton and Ashkan Soltani. (31 October 2013). "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *The Washington Post.*

Geraghty, Tony. (1981). *Who Dares Wins: The Story of the Special Air Service, 1950–1980.* Tiptree Essex: Anchor Press.

Greenwald, Glenn. (31 July 2013). "XKeyScore: NSA Tool Collects Everything A User Does On The Internet." *The Guardian.*

Herman, Michael. (1996). *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Herring, Jan P. (1999). "Key Intelligence Topics: A Process To Identify and Define Intelligence Needs." *Competitive Intelligence Review* (10:2) 4–14.

Hulnick, Arthur S. (1996). "The Uneasy Relationship Between Intelligence and Private Industry." *International Journal of Intelligence and Counter-Intelligence* (9:1) 17–31.

Hulnick, Arthur S. (1991). "Intelligence Co-operation in the Post-Cold War Era: A New Game Plan?" *International Journal of Intelligence and Counter-Intelligence* (5:4) 455–465.

Internet World Stats. (30 June 2012). *Internet Usage Statistics: World Internet Users and Population Stats.* [http://www.internetworldstats.com/stats.htm] last accessed 1 September 2013.

Kamil, Fred. (1979). *The Diamond Underworld.* London: Allen Lane.

Kaplan, Andreas M & Michael Haenlein. (January–February 2010). "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons* (53:1) 59–68.

Kemp, Anthony. (1994). *The SAS: Savage Wars of Peace*. London: John Murray.

Krizan, Lisa. (June 1999). *Intelligence Essentials For Everyone.* Occasional Paper Number 6. Washington DC: Joint Military Intelligence College.

Liaropoulos, Andrew, N. (June 2006). *A (R)evolution In Intelligence Affairs? In Search of a New Paradigm.* Research Institute for European and American Studies. Research Paper No 100.

Madsen, Wayne. (1999). *Genocide and Covert Operations in Africa, 1993–1999.* New York: Edwin Mellen Press.

Madsen, Wayne. (1993). "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counter-Intelligence* (6:4) 413–488.

Michaels, Jon D. (31 August 2008). "All The President's Spies: Private-Public Intelligence Partnerships in the War on Terror." *California Law Review.* ((96:4) 901–966.

Miller, Michael C. (2007–2008). "Standing in the Wake of the Terrorist Surveillance Program: A Modified Standard for Challenges to Secret Government Surveillance." *Rutgers Law Review* (60) 1039.

Newkirk, Anthony B. (2010). "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance After 9/11." *Surveillance and Society* (8:1) 43–60.

Ng, Eddy S W, Linda Schweitzer & Sean T Lyons. (2010). "New Generation, Great Expectations: A Field Study of the Millenial Generation." *Journal of Business Psychology* (25) 281–292.

Prados, John. (2006). *Safe For Democracy: The Secret Wars of the CIA.* Chicago: Ivan R Dee.

Priest, Dana & William Arkin. (19 July 2010). "The Growth of Top Secret America." *The Washington Post*. [http://projects.washingtonpost.com/top-secret-america/] last accessed 1 September 2013.

Prunckun, Hank (2013). Personal conversation on August 8, 2013, Canberra, Australia. I am very grateful to Dr Prunckun for pointing out this issue regarding intelligence tradecraft.

Risen, James. (16 April 2000). "Secrets of History: The CIA in Iran." *The New York Times.*

Schlesinger, Stephen & Stephen Kinzer. (1999). *Bitter Fruit: The Story of the American Coup in Guatemala*. Cambridge, Mass: Harvard University Press.

Shearer, David. (1998). *Private Armies and Military Intervention.* Adelphi Paper 316, International Institute of Strategic Studies.

Shelley, Louise. (Winter 1995). "Transnational Organised Crime: An Imminent Threat to the Nation-State?" *Journal of International Affairs* (48:2) pp 463–489.

Shorrock, Tim. (2008). *Spies For Hire: The Secret World of Intelligence Outsourcing.* New York: Simon & Schuster.

Sillitoe, Sir Percy. (1955). *Cloak Without Dagger*. London: Cassell and Company Ltd.

Silverstein, Kenneth. (28 July 1997). "Privatising War: How Affairs of State Are Outsourced to Corporations Beyond Public Control." *The Nation.*

Smith, Woodruff, D. (1982). *European Imperialism in the 19th and 20th Centuries.* Chicago: Nelson-Hall.

Steele, Robert David. (February 2002). *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Non-Traditional Threats.* Studies in Asymmetry. Carlisle, Pa: Strategic Studies Institute, US Army War College.

Steele, Robert David. (May 1998). "Open Source Intelligence: Private Sector Capabilities to Support DOD Policy, Acquisitions and Operations." *Defense Daily Network Special Report.* [http://www.fas.org/irp/eprint/oss980501.htm] last accessed 1 September 2013.

Steele, Robert David. (1995). "Private Enterprise Intelligence: Its Potential Contribution to National Security." *Intelligence and National Security* (10:4) 212–228.

Straw, Joseph. (2013). "Smashing Intelligence Stovepipes." *Security Management.* [http://www.securitymanagement.com/article/smashing-intelligence-stovepipes] last accessed 1 September 2013.

The Australian. (10 August 2012). "Google Fined $21.3m For Breaching Privacy of Apple Safari Users."

The World Bank. (2012). *Maximising Mobile: 2012 Information and Communications for Development.* Washington DC: The World Bank. [http://siteresources.worldbank.org/ExtInformationAndCommunicationAndTechnologies/Resources/IC4D-2012-Report.pdf] last accessed 1 September 2013.

Todd, Paul & Jonathan Bloch. (2003). *Global Intelligence: The World's Secret Services Today*. London: Zed Books.

Treverton, Gregory F. (2003). *Reshaping Intelligence for the Information Age.* Cambridge: Cambridge University Press.

Troy, Thomas F. (1991). "The "Correct" Definition of Intelligence." *The International Journal of Intelligence and Counter-Intelligence*. (5:4) 433–454.

Unsinger, Peter Charles. (1999). "Meeting A Commercial Need For Intelligence: The International Maritime Bureau." *The International Journal of Intelligence and Counter-Intelligence* (12:1) 58–72.

Voelz, Glenn J. (June 2006). *Managing the Private Spies: Use of Commercial Augmentation for Intelligence Operations*. Washington DC: Joint Military Intelligence College.

Warner, Michael. (2007). "Sources and Methods for the Study of Intelligence." In Johnson, Loch K. (Ed.) *Handbook of Intelligence Studies.* Abingdon, Oxon: Routledge.

Wong, Katherine. (2006). "The NSA Terrorist Surveillance Program." *Harvard Journal of Legislation.* (43:2) 517–534.

Wright, Jeffrey W. (1991). "Intelligence and Economic Security." *The International Journal of Intelligence and Counter-Intelligence* (5:2) 203–221.

ABOUT THE AUTHOR

Dr Ruth Delaforce is a lecturer with the School of Criminology and Criminal Justice, and adjunct investigator with the Australian Research Council, Centre of Excellence in Policing and Security, at Griffith University. She has previously been employed in the private and public sectors, and law enforcement. Her research interests include the military-crime nexus, private military and security companies, insurgency and counterinsurgency studies.

- o O o -

Research Article

Combating Political Police: An Overview of National Action's Counterintelligence Program 1982–1990

Troy Whitford[§]

During the mid to late 1980s the radical nationalist group National Action was targeted by domestic intelligence agencies. Known as "Operation Odessa" it was part of Australian Security Intelligence Organisation's program to combat what it saw as a rise in politically motivated violence. ASIO and state police Special Branch officers placed the group under surveillance and sent agents to disrupt meetings and recruit informants. Concurrently, National Action had developed its own counterintelligence program structuring the group in an effort to preserve secrecy, educating its membership in situational awareness and designating a senior member as an intelligence officer. Ultimately National Action counterintelligence program was unable to match the highly resourced government agencies and internal discipline issues meant the group was eventually disbanded. However, National Action's effort to develop a counterintelligence program provides some examples of what low resourced Issue Motivated Groups are capable of achieving.

Keywords: Human intelligence (HUMINT), counterintelligence, issue motivated groups (IMG), National Action, radical nationalists, Australian Security Intelligence Organisation (ASIO).

INTRODUCTION

The capacity of small political organisations or issue motivated groups (IMGs) to disguise their activities from larger organisations or governments is in part contingent on those groups developing counterintelligence programs. This may involve educating the membership on the threats posed by larger

[§] Corresponding author: twhitford@csu.edu.au

organisations or governments, developing a culture of situational awareness and establishing protocols for communication between members.

Using the radical nationalist group National Action as an historical example it is possible to explore some of the ways IMGs could develop counterintelligence methods. National Action is a suitable study because it was subject to investigation by domestic intelligence services in the mid to late-1980s and documented evidence is available on its counterintelligence methods. Further, National Action was operating in a period prior to modern technologies such as the internet and social media. The absence of such communication technology meant a greater emphasis was placed on human intelligence gathering or human intelligence sources (HUMINT).

The Australian Security and Intelligence Organisation (ASIO) was and still is the primary agency charged with gathering intelligence on IMGs or politically motivated violence (PMV) in Australia. However, state police Special Branches also have a role in gathering intelligence. In some respects there is an overlap of roles between state police and ASIO (James, 2005), but it can be best defined along the lines of ASIO collecting intelligence as a pre-emptive measure and the state police investigating with respect to breaches of criminal codes (James, 2005).

This division is apparent in the National Action narrative. ASIO had tended to use electronic surveillance and human intelligence in an attempt to learn about and disrupt the group's activities. State police, particularly Special Branch were more concerned with actual crimes committed and approaching members to inform on other members regarding criminal activities. As this article illustrates the two approaches to monitoring this particular IMG proved complimentary as it was ASIO's electronic surveillance that unwittingly assisted in the conviction of a murder of one of National Action's members.

While a brief background is provided for contextual reasons it is not the scope of this study to assess the politics of National Action or tell its history. The history of National Action has been documented by its founder Dr Jim Saleam and is featured in a number of articles and texts. National Action's formation, ideology and contribution to the Australian political landscape can be found in Saleam's doctoral thesis, *The Other Radicalism: An Inquiry into Contemporary Australian Extreme Right Ideology, Politics and Organisation 1975–1995* (1999). Further studies include *A Political History of National*

Action: Its Fears, Ideas and Tactics (Whitford 2011) and *All In The Name of Human Rights: An Historical Case Study on Australian Nationalism and Multiculturalism, 1980–1990* (Whitford 2012).

This historical study is solely focused on National Action's counterintelligence program albeit ultimately unsuccessful against better resourced and technologically advanced domestic intelligence services. National Action's approach to counterintelligence provides an interesting insight into how IMGs may operate in developing an effective intelligence and counterintelligence facet to their organisation. The article does not aim at providing direction for intelligence agencies in investigating IMGs, but rather illustrates how at least one IMG had attempted to develop its own intelligence capacity. This modest contribution to the literature on IMGs and counterintelligence looks at the issue from the perspective of National Action without applying the usual political biases which tend to inhibit a better understanding of the operations and tactics of these kinds of groups.

BACKGROUND

In a contemporary sense National Action could well be described as an Issue Motivated Group (IMG). Initially based in Sydney the radical nationalist group was established in 1982, by seventeen people. Its numbers increased over the 1980s and eventually had a membership of over 500 and branches in Sydney, Melbourne, Brisbane and Adelaide. National Action saw itself as a militant propaganda unit protesting against immigration, multiculturalism and globalisation. Its founder Jim Saleam structured the group on a small executive management supported by an inner membership that would undertake the bulk of the group's activities and an outer group of supporters. The structure was designed to enforce an authoritarian leadership to foster internal discipline and counter infiltrators.

National Action came to the attention of domestic intelligence services ASIO and NSW police Special Branch early in its formation. Changes to racial discrimination laws during the 1980s had criminalised many of the propaganda activities of National Action and it in response tended to move toward more confrontation tactics. In 1984, members of National Action stormed the offices of Macquarie University's Student Council after it had been attacked by pro multicultural groups and barred from campus (*Sydney Morning Herald*, 24 March 1984). Later in the same year, an organiser for the Combined Unions

Against Racism (CUAR) had their car fire bombed and claimed it was orchestrated by National Action (*Ultra* 1984).

In 1989, National Action attacked the Offices of the Antidiscrimination Board in Sydney and a meeting of the NSW Liberal Party (*Ultra* January 1989). Links were also made between National Action and Jack Van Tongeren a West Australian based neo-Nazi who was charged with arson, conspiracy to commit arson and break and enter after a number of Chinese restaurants were fire bombed (*Sydney Morning Herald* 19 February 1989). Simultaneously, National Action were also deliberately creating a mystique around itself starting rumours it had connections to extreme right wing overseas organisations such as the French Party of New Forces and the South African Afrikaner Resistance Movement (Saleam, 1999).

Rumours that National Action had access to firearms also increased domestic intelligence services' interest in the group. The violence surrounding National Action peaked in 1989 when two of its members fired a shot gun shot into the home of Eddie Funde, the Chief Representative of the African National Congress. The two assailants were charged along with Jim Saleam. Saleam denied any part in the crime but was convicted for providing the shot gun to the two members.

Mostly attributed to National Action the spate of right wing violence taking place in Australia during this period saw the Human Rights Commission announce an inquiry into racist violence. Further, National Action was named in Parliament by the then-Prime Minister Bob Hawke as a "threat to the social cohesion" of Australia (Hawke, 1989). Responding to political concerns NSW Special Branch officers and ASIO officers launched Operation Odessa which involved infiltrating National Action's meetings to disrupt and inform on the membership, surveillance of the group's activities and leadership and the instillation of listening devices at National Action's headquarters.

Operation Odessa was part of a larger strategy to address what ASIO perceived as an escalation in violence from right wing groups (ASIO, 1990). Through its Politically Motivated Violence Program, ASIO claimed it had operational success in curbing the work of violent racist groups and its investigation in conjunction with state police had led to a number of arrests (ASIO 1991) notably Jim Saleam and members of National Action. Further, in 1991, prosecutions of a shooting murder which had taken place at National

Action's headquarters were assisted by recordings made by ASIO. Officers had actually recorded an altercation between two members of the group and the subsequent shooting (Fife-Yeomans, 1991).

DEVELOPING A COUNTERINTELLIGENCE PROGRAM

Since its inception National Action had viewed itself outside of Australia's political mainstream and viewed the established political apparatus as a combative. Early in National Action's formation "secrecy" was an important facet to its operation. In one of its early manifestos *What is to be done?* (1985) Saleam wrote secrecy would be an important part of the organisation. He understood that if the organisation grew into a mass movement that general secrecy would be difficult to maintain but it could still be applied to key sections of the organisation.

Secrecy about the operations of the National Action, according to Saleam, was the best defence against the 'political police' in their efforts to infiltrate the group or gather intelligence. In National Action's manifesto Saleam remarked that early attempts by NSW Special Branch to investigate National Action had failed and officers had remarked that it was National Action's secrecy which made investigations difficult (Saleam 1985).

Enforcing secrecy was an organisational structure which favoured a hierarchy of members and supporters. A supporter was seen as a person of loose commitment to the organisation while a member was more trusted and proven in their commitment to National Action. Information regarding National Action's activities and program would be reserved for members. Secrecy was also enforced within the general rules of conduct for members and supporters. For example, it was required at general meetings members and supporters would not discuss their occupations, sources of income, or personal affairs; nor would they share full names and addresses (National Action, 1987).

Educating the membership on the intelligence threats to National Action was another key element to its counterintelligence program. In 1987, Saleam wrote an extensive pamphlet on dealing with domestic intelligence services. He highlights ASIO, the federal police and Special Branches as performing intelligence gathering activities on political organisations. The pamphlet then provided scenarios on how members or supporters of National Action could be approached by domestic intelligence services. The pamphlet emphasised that members and supporters would often be approached with threats of criminal

charges or given information about the group's leadership in an effort to create doubt and division in the mind of the activist.

In addition to general warnings and background to police activity some fundamental practical measures were highlighted and members were encouraged to adopt them. Some of the measures included hiding membership lists and contacts, never bulk mailing organisational mail from the same post office, avoiding business discussions on the telephone, reducing paperwork and destroying processed mail. It was also stressed that vehicles should not be parked near meeting venues as intelligence officers often made note of registration plates. National Action also encourage its members to be suspicious of new members or supporters particularly those that may advocate violence as they may be a provocateur (Saleam 1985).

NSW Special Branch had acknowledged that National Action developed a sophisticated intelligence network. In the pre information technology age, National Action had created extensive index systems including the names and addresses of politicians, police and media (Harvey, 1989). National Action had also developed an executive position within the group serving as an intelligence officer. The position was developed as early as 1984 and involved the vetting of new members or supporters in an effort to assess if they were infiltrators or informers for government intelligence officers or even opposition groups.

The leadership was acutely aware of the damage informers and infiltrators could have on the group. An important part of National Action's counterintelligence program was monitoring new members and supporters for signs of connections with Special Branch or ASIO officers. According to National Action documents, several attempts at infiltration or efforts to recruit National Action supporters as operatives had been undertaken by ASIO and Special Branch police.

A key infiltrator and subsequent informer later referred to as CC18 during the 1994–1997 Royal Commission into New South Wales Policing is an ideal example on how intelligence agencies were able to exploit division within National Action and weaken the movement. CC18 was associated with National Action from September between 1983 until April 1985. According to Saleam, CC18 had approached the group with ambitions of taking over the leadership and steering it toward more neo-Nazi ideals (2003).

Nevertheless, his attempts proved unsuccessful and he had a violent altercated with one of National Actions members. NSW Special Branch had learnt of the altercation and approached CC18 in an effort to recruit him as an informer. CC18 would regularly make contact with a Special Branch officer over the telephone and provide that officer with information regarding activities of the group but it was not until 1989 he was formally recruited as an informer (Saleam, 2003).

To combat informers National Action's intelligence officer had adopted an internal surveillance method when assessing its new members. The officer would organise new members or supporters to be placed alongside trusted members when the group were distributing literature, hanging posters or attending protests. The aim was to monitor the behaviour and conversations of the new member and report back to the intelligence officer and the group executive. The new member would be assessed for the kind of conversations they would have with their mentor and also to assess their position on a range of political views.

In addition to vetting new membership the intelligence officer also collected substantive subject files on other groups and individuals perceived as threats to National Action. With greater access to personal computers the group also established extensive databases of information using their subject files and electorate rolls. The intelligence officer was also responsible for ensuring the groups important documents were spread out in a few different locations. Full membership lists and other material deemed "classified" were never kept at the group's headquarters (Saleam 2013).

National Action also had concerns about electronic surveillance early on. As a basic means to counter electronic surveillance they developed the "burning bin." As the name suggests members had simply used a steel rubbish bid and would write down on paper the conversations they wanted to have in private and then burn each piece of paper after it was read by the other party. National Action also removed the telephone from the wall at headquarters during meetings or discussions. However, on the night of the shooting murder this protocol was not observed (Saleam 2013).

Not all the counterintelligence measures were defensive. As a means of identifying individuals in opposition groups National Action's intelligence officer would organise its members to visit the meeting locations of opposition

groups and copy down car registration numbers. Prior to 1990, it was possible to get the details of an individual by requesting it from the Roads Traffic Authority. A person seeking details of an individual could supply the registration number of the vehicle, pay a small administrative fee and receive the name and address of the owner of that vehicle.

A key success to National Actions counterintelligence program was its tactic of publicising interactions with intelligence officers. National Action advocated that if approached by domestic intelligence services, members were encouraged to first provide misinformation through simple lies. Secondly, where possible members were also asked to photograph intelligence officers and put names to the photographs. Finally, they encouraged members to gather details of the intelligence officers who approached them and publish the Officer's details along with photographs. The strategy was to name lead intelligence officers, what they had said to National Action members and achieve maximum coverage from the media in order to expose ASIO and Special Branch operations (Saleam 2013).

GATHERING AND UTILISING ITS INTELLIGENCE

Obtaining details on intelligence officers and members of state police as well as the Special Branch fed National Action's more aggressive counterintelligence measures. In 1989, a Sydney Morning Herald journalist reported that National Action had mailed a three page letter to the home addresses of NSW police officers. The letter suggested that the Special Branch had been requested to undertake the anti-racism cause and was 'out to get anyone who is pro-Australian and opposed to Asian uncontrolled immigration' (Harvey, 1989).

The letter continued to assert there was a liaison between Special Branch, the Gay and Lesbian Immigration Task Force and Sydney Anti-apartheid activist Rev Dorothy McMahon. However, for many the contents of the letter campaign were of less interest than the ability of National Action to obtain the names and private addresses of NSW police officers. According to the media report officers were distressed at the prospects that a radical group such as National Action was able to gather their personal details.

National Action's intelligence gathering capacity also assisted it in its anti-media campaign. After National Action had unsuccessfully lodged a number of complaints to the Australian Press Council for unfair or erroneous reporting it used its intelligence network to find the names addresses and telephone numbers

of targeted journalists. The personal details of those journalists were published in National Action's journal and subsequently they received threats via mail and telephone. At one juncture, a journalist working for *A Current Affair* had her home picketed by National Action members after the journalist had earlier filed a story on the group and allegedly invaded the privacy of National Action members (Whitford, 2011).

National Action's intelligence networks also extended to the Sydney taxi industry. During the late-1980s National Action had embarked on a propaganda campaign to highlight the rise in immigrants working as taxi drivers in Sydney and contended that these drivers were working longer hours and without holiday or sick pay benefits. The inference was that European drivers where being pushed out of the industry in favour of other ethnic groups.

In response to its concerns of corruption in the taxi industry and anxieties that it had become too orientated toward migrants, National Action embarked on an intelligence gathering operation to expose immigrant drivers. It had been able through its network to collect the taxi licence numbers, and ethnic backgrounds of those driving taxis in Sydney. Over a short period of time National Action compiled a list of almost 200 drivers. The driver's ethnic appearance, taxi licence numbers and the company they worked for were printed in a publication titled *Taxi-Gate: Cheap Labour and Corruption in the Taxi Industry* (1988). The publication also stated that it would locate and publish the names and addresses of those they believed were corrupting the taxi industry.

More intriguing is the possibility that National Action had also been effective in getting information from intelligence agencies. In a document entitled *The Security Question* (n.d.) there is reference to a meeting between ASIO, the Victorian Counter Terrorism Unit and NSW Special Branch that took place in May or June 1990. According to the document the meeting was to review the information these bodies had gathered on National Action including divisions within the group. The document also suggests that a Special Branch officer had told a female associate of National Action the name of an informer within National Action ranks.

There are two likely interpretations of this anecdote; first the Special Branch officer may have been spreading disinformation about the meeting between intelligence agencies and perhaps deliberately named the informant as a means to incite greater disharmony in the group. Second, National Action may

have had some ability in extracting information from intelligence officers. Regardless of the interpretation what remains clear is the interplay of intelligence gathering and counterintelligence between government agencies and National Action.

ASSESSMENT OF NATIONAL ACTION'S COUNTERINTELLIGENCE PROGRAM

National Action appears to have had some success in their ability to exploit its networks and gather information. It is difficult to gain a clear view of the extent and range of its network of information as historical sources are very narrow—but National Action's ability to locate journalists and police certainly demonstrate an intelligence capability.

As stated earlier, a substantial part of National Action's counterintelligence program was fundamental secrecy, but, as National Action grew in size and notoriety secrecy proved more difficult to manage. Despite protocols and an organisational framework designed to keep secrecy it was unable to develop a disciplined membership and supporter base. It appears the vetting process introduced by National Action—the decision to align new members or supporters with more trusted members and then essentially report back to National Action's executive on behaviours and political outlooks was not affective in the long term. National Action had difficulty in identifying which members would be effective 'political guerrillas' and which were essentially just thugs.

The dispute between National Action members at its headquarters (recorded by ASIO listening devices in 1991) that ended in a shooting death is just one example of the undisciplined violent influence which had consumed the group. Another type of person attracted to National Action were young men often of middle and working class backgrounds who felt marginalised and disaffected from society (Moore 2005). A membership comprising of even a few such people may have proven an asset for intelligence agencies seeking informants but from National Action's perspectives these kinds of individuals were security risks.

CONCLUSION

National Action had certainly developed an intelligence program that made use of extensive human intelligence contacts to develop a network of information

gathering that was able to 'shock' media and law enforcement. It had made use of open source information and conducted covert surveillance as a means to protect its interests. Its membership was educated in situational awareness and practical measures for developing a culture of secrecy.

The establishment of an intelligence officer position within the group also illustrates an understanding by National Action that collecting and protecting information was a significant part of the group's operation. Another facet to its program was the conscious decision to make public every encounter it had with intelligence agencies therefore reducing the capacity of Special Branch and ASIO to undertake covert activities.

After eight years National Action was ultimately, disbanded and its key personnel were imprisoned in part due to the role of intelligence agencies. But as an historical example, National Action's counterintelligence methods illustrate the possibilities for low resourced IMGs. Any group that adopts a degree of intelligence capability along with principles of secrecy, situational awareness and proactive information gathering techniques can aim to protect its interests against Government intelligence agencies or oppositional groups.

REFERENCES

Australian Security Intelligence Organisation, (1990). *Report to Parliament 1989–90*, Canberra: Australian Government Printing Service.

Fife-Yeomans, J, (1991, June 26). "Hey Smith, You're Dead, Dead, Dead, Dead, *Sydney Morning Herald.*

Harvey, S, (1998, March, 25). "Police Get Extremist Hate Mail at Home," *Sydney Morning Herald*.

Hawke, R, (1989, April, 5). House of Representatives Commonwealth Parliament Hansard.

James, S, (2005). "The Policing of Right-Wing Violence in Australia," *Police Practice and Research: An International Journal*, 6, 103–119.

Moore, A, (2005). "Writing About the Extreme Right," *Australia, Labour History*, 89, 1–15.

Saleam, J, (1985 December). "What is to be Done? In-house publication by National Action.

Saleam, J, (1987, June). How to Combat the Political Police. In-house publication by National Action.

Saleam J, (1999). *The Other Radicalism: An Inquiry Into Contemporary Australian Extreme Right Ideology, Politics and Organization 1975–1995,* PhD Thesis, University of Sydney.

Saleam, J, (2003). "Enemies of the State: The State Conspiracy Against National; Action and Australian Nationalist's Movement 1988–1991. http://home.alphalink.com.au/~radnat/conspiracy.html date accessed 2 October 2013.

Saleam, J, (2013, September,29). Personal communication with author.

Saleam, J, (n.d.). Letter to Victorian Branch entitled "The Security Question, National Action correspondence with membership."

Sydney Morning Herald, (1984 March 24).

Sydney Morning Herald, (1989 February 19).

Ultra: Internal Bulletin of National Action, (1984). Trial by Media Special Issue.

White, I.M & Wong U.R [sic], (1998). *Taxi-Gate: Cheap Labour and Corruption in the Taxi Industry*. National Action.

Whitford, T, (2011 April). "A Political History of National Action: Its Fears, Ideas and Tactics," *Rural Society* Vol. 20: 2, 216–226.

Whitford, T, (2012). "All in the Name of Human Rights: An Historical Case Study on Australian Nationalism and Multiculturalism," in Nationalism and Human Rights, *Theory and Practice in the Middle East, Central Europe and the Asia-Pacific*, Grace Cheng, ed., South Yarra, Victoria: Palgrave Macmillan.

ABOUT THE AUTHOR

Dr Troy Whitford lectures in history and politics at Charles Sturt University and is a doctoral supervisor at the Australian Graduate School of Policing and Security. His research interests include political intelligence gathering and the place of private investigation firms within the broader intelligence community. Dr Whitford has written on elements of the extreme right in Australia and the nature of political intelligence in the Twenty-First Century. He is a government licensed private investigator and a director of Civintel Pty Ltd, an intelligence-led private investigations company.

- o O o -

Research Article

INTELLIGENCE: A RISK TOO FAR, OR "DIGNITY AND JUSTICE FOR ALL OF US"?

Alan Beckley[**]

This study takes the form of a critical discussion that examines the growth of surveillance and intrusion into the privacy of Australian citizens for the ostensible purpose of gathering intelligence and maintaining security. It investigates the history of the growth of surveillance during the last decade and comments on the intrusion on privacy by public sector organisations, but mainly focuses on the growth in data harvesting carried out by private sector or quasi-governmental outsourced organisations while noting the lack of accountability of such agencies. It examined the level of intrusion, the possible uses of the data, along with outcomes and issues of incursion into citizens' privacy. The study analysed selected cases were data had been gathered by some (but not all) modern methods of gathering intelligence, such as closed circuit television (CCTV); travel and transport; private communications, social media; DNA sampling and databases. It quantified the effects of intelligence gathering, identifying and analysing cases where organisations had exceeded their powers in obtaining data and recommended several means of ensuring proper accountability and the implications for government policy.

Keywords: intelligence; privacy; CCTV; telephone-tapping; social media; DNA

INTRODUCTION

This critical discussion is intended to stimulate debate regarding the justification of gathering intelligence for a variety of purposes, the necessity to gauge its value to society and that the value should be balanced against its effects on the privacy of the individual citizen. The interpretation of the term *intelligence* in this context means sensitive and intimate personal data that is

[**] Corresponding author: a.beckley@uws.edu.au

being collected relating to the private lives of individual citizens in Australia. Intelligence is being gathered by both private and public organisations in an ever-increasing variety, intensity and depth. It should be noted that this study is mainly focused on intelligence gathering by private sector organisations; therefore readers should gauge its contents as only a partial discussion of the entire situation.

Developments in the power and speed of information communication technology have enabled the opportunity to build databases linking intelligence and data of private information about individual citizens, facilitating cross-referencing to identify personal traits and attributes to build a lifelike "virtual" portrayal of the person. The discussion suggests that information gatherers should be vigilant and conscious of their intrusions into personal privacy and be held accountable to justify their reasons and purpose for collection of such data. Legitimate investigatory agencies that are legally empowered to collect personal data such as criminal intelligence should confirm their operatives are aware of the responsibilities to cause as little intrusion in the lives of the citizens as possible along with the maximum attention to safeguard sensitive personal data and ensure confidentiality (Beckley, 2000: 18).

This critical discussion will first examine some recent developments in law and practice and then investigate techniques to manage the impact and risk of intelligence gathering. It will discuss the actual situation regarding the operations of closed circuit television (CCTV); transport and travel; personal communications and social media; and collection of DNA (deoxyribonucleic acid) samples and databases. By drawing the effects of these areas together, the reader can make a judgement on the overall intrusion into their privacy from these examples. It should be noted that these forms of intrusion are only examples and are not an exhaustive examination of all the means of intrusion into the privacy of citizens in democratic societies. The discussion has used a specific definition of *intelligence* for the purpose of inclusion of the private and public sectors:

> A value-added product, derived from the collection and processing of all relevant information relating to client needs, which is immediately or potentially significant to client decision-making (ACS, 2000: 15).

Therefore *intelligence* can be viewed from the different perspectives of criminal intelligence or data for the purposes of customer relationship management (CRM) informing suppliers of retail customers' needs and requirements. Whatever the purposes of gathering intelligence, it inevitably leads to intrusion into the privacy or bodily integrity of the individual citizen, but most countries have statutes, rules and regulations about the collection, recording and dissemination of intelligence for police, law enforcement or security purposes. The states and territories of Australia have different legal frameworks in relation to human rights and fundamental freedoms, but the country as a whole is signed up to relevant Treaties (Gans, Henning, Hunter, Warner, 2011: 9–10) that respect and protect the right to private and family life (for example: International Covenant on Civil and Political Rights (ICCPR) came into force in Australia 13 November 1980—enacted in Australia as the *Privacy Act 1988*). Australia also recognises the *Universal Declaration of Human Rights* (UN, 1948) which although not a treaty, is regarded as an important reference point on citizen rights (Gans, et al., 2011: 10); it states:

> The United Nations Universal Declaration of Human Rights (1948)—Right to Privacy
>
> Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (UN, 1948)

The months of June to August of 2013 were especially influential in providing information internationally about data collection and security intelligence on individual citizens by governments. This period included the trial of Bradley Manning, (a low-level intelligence operative employed in the US military) in the so-called "Wikileaks" incident, who pleaded guilty to the release of classified information into the public domain that resulted in intense media scrutiny (for example: McGeough, 2013, July20). The military court which tried him suggested he could be imprisoned for up to 136 years for leaking 700,000 diplomatic and security documents.

Also, an-ex National Security Agency (NSA) contractor Edward Snowden admitted leaking information to international media sources about the "Five Eyes" nations (Australia, Canada, New Zealand, the United Kingdom, and the United States). These partners have access to an information technology system

called *PRISM* which is able to scrutinise and analyse most electronic messages and on-line activities to produce intelligence reports for national security purposes. The NSA is able to trace telephone calls and store the telephone numbers of citizens without their knowledge or consent (Dorling, 2013).

These announcements and developments have caused concerns to citizens regarding the privacy and confidentiality of their personal details. Indeed, many politicians have questioned the need for this extreme level of intrusion (Risen, 2013), although an ex-chief of the NSA was quoted as saying that "spying on citizens' web activity [was] good news" (Gallagher, 2013). At the time of writing these are recent disclosures and it will take some time for protests against intrusion to prevail and legislation to respond, depending on the strength of public opinion pressure. This is clearly the age of surveillance on the citizen, from their private communications to their activities in public spaces covered by CCTV.

CLOSED CIRCUIT (CCTV)

Beckley (2002) published a journal article on the subject of the proliferation of CCTV in the UK, but by 2012 the number of cameras had trebled (McCahill & Norris, 2012: 6) and was estimated to be "at least" 4 million (Porter, 2009: 11). However, the Director (Alex Deane) of "Big Brother Watch," the organization which carried out the camera survey, said: "The evidence for the ability of CCTV to deter or solve crimes is sketchy at best" (BBC, 2009). Local councils and the police say that the cameras help to cut crime (AIC, 2009), catch criminals and lower the levels of the fear of crime (Anderson & McAtamney, 2011). Indeed, some research (Welsh & Farrington, 2008) suggested that crime can be reduced by 51% in car parks and 23% on public transport by the use of CCTV.

An evaluation report on Perth Transport Authority claimed a 50% reduction in assaults on trains covered by CCTV (WA Auditor General, 2011). Also, members of the public appear to support the introduction of CCTV (Bennett & Gelsthorpe, 1998; Ditton, 1998). There is conflicting evidence to support the cases for or against CCTV, despite considerable academic research (Pointing, 2012). In the case of the specific incident of the London transit bombings in July 2005 (Brooks & Corkhill, 2012: 58) it was stated that data from CCTV proved to be "an effective and valuable source of information in the investigation" (Bloss, 2009: 235). Also, in the case of Jamie Bulger, a toddler

who was abducted and murdered in Liverpool (UK), the perpetrators would not have been identified without the benefit of CCTV cameras (Scott, n.d.).

In Australia, the number of CCTV systems has been described as "more restrained than the UK" (Sutton & Wilson, 2004: 312), but in 2003, it was said (Wilson & Sutton, 2003: 5), "With systems already established in all Australian capital cities except Darwin, future expansion is likely to be in regional centres and suburban locations. Digital technology is also likely to become the industry standard." Cubbage (2012: 55) reported that the CCTV cameras in Australia are not so state-of-the-art, lacking high definition, precision and operability, thereby making identification of suspects more difficult. But projects are proposed (Carnovale, 2011) to combine CCTV with facial recognition systems (McDevitt, 2010) which may be more effective crime detection/prevention measures (Cameron, 2011) although it has taken a considerable time to develop the technology. The detection of a crime of murder in Victoria was mainly due to a CCTV recording (Dowsley & Flower, 2012) from a shop which viewed passers-by on the footpath outside, which could have been unlawful (Arnold, 2008). The video material, when transmitted on television, led directly to the arrest of the person subsequently found guilty of the crime (Silvester & Butt, 2012).

Although most CCTV operations are for laudable and sound reasons, the majority of the establishments in this field are private or outsourced organisations staffed by private operatives observing their community and its inhabitants from remote locations. This can lead to unapproved and unwarranted intrusion into the private affairs of individuals especially when cameras are used over-zealously or data is shared without proper authority or control and with little or no accountability. The focus of the critical discussion will now turn to transport and travel.

TRANSPORT AND TRAVEL

Automatic Number Plate Recognition

There is a similar situation between the UK and Australia with CCTV on traffic cameras or automatic number plate recognition (ANPR) systems; that is, where the UK leads, Australia appears to follow. In the UK, the National Policing Improvement Agency, whose operational responsibility in 2012 was handed over to the UK Home Office, received 15 million ANPR records per day (NPIA, 2012). The ANPR system is to be further rolled out throughout the UK from its concentration on motorways and ports and borders because of its positive

outcomes on the "fight on crime." For example, in the year 2006–2007, ANPR led to: "the arrest of 20,592 individuals; the identification of 52,037 vehicle related document offences; the seizure of 41,268 vehicles for document offences; the identification and recovery of 2021 stolen vehicles" (NPIA, 2012).

Sophisticated cameras are able to record the registration number of motor vehicles and track their journeys all over the country; the system is able to produce warnings and alerts to police officers thereby reducing crime and enhancing police officer safety. However, in Australia, according to Clarke (2009: 47):

> Australian policing agencies have been variously piloting and deploying ANPR, but without public oversight or control. A national agency, Crimtrac, is proposing to develop a vast database, which would store billions of entries showing the whereabouts of vehicles about which no suspicion of wrongdoing exists. Its purpose is expressly to facilitate mass surveillance of the Australian population. This represents national security extremism, and is a gross breach of trust by law enforcement agencies in Australia.

The records from ANPR were originally to be retained for 2 years (Watson & Walsh, 2008), but this, in 2006, was extended to 5 years; from its stated intention to be a counter terrorist measure it suffered from "function creep," and it is now a law enforcement aid. Indeed, Watson & Walsh, (2008: 4) describes ANPR in Australia thus: "This is a very large tool being used to monitor a very small percentage of the population, whilst containing a great deal of information about every person in the country."

The Federal Privacy Commissioner had previously commented on the plan: "The Office would caution against establishing infrastructure that could be used in such an expansive and invasive manner" (OFPC, 2008: 7). Crimtrac (McDevitt, 2010) proposed a network of about 100 fixed and additional mobile and in-vehicle ANPR linked cameras feeding into a national recording system. McDevitt (2010: slide 6) also stated that ANPR system tracks "vehicles not people" with tripartite benefits to traffic, law enforcement and national security.

From the traffic point of view, there are many advantages in using cameras to prevent "red-light running" especially in targeted road junctions with the highest number of offences. In the UK, red-light running results in 4,000–5,000

injury road collisions per year (Lawson, 1991). In terms of financial costs, according to research completed by Ayuso, et al. (2009) in Europe slight injury road traffic collisions cost the equivalent of A$71,000 and fatal incidents slightly over A$1m. Although some aspects of monitoring of traffic can be justified on the grounds of road safety, and the equipment is managed by publicly accountable bodies, there does not appear to be a rational explanation for the extent and volume of the data being collected, and thus its proportionality regarding the invasion of citizens' privacy.

Security Monitoring of Public Transport/Transit Areas

In response to the US-led program (US-VISIT) of biometric, physical and documentary profiling for foreign visitor surveillance; (Bloss, 2009; Goold, 2010) many other countries, including Australia are following suit, although the security in this area is provided and managed by private out-sourced companies or quasi-governmental organisations.

Australia invested A$69m to enhance immigration systems with a biometric-based visa system (fingerprint and facial images) from visa applicants from ten overseas locations, to "reduce the risks of terrorists, criminals and other persons of concern" (DPMC, n.d.) from entering Australia. In an audit of the management of the Department of Immigration and Citizenship (DIAC) the Auditor-General reported that the "benefits of biometrics in the area of border security generally relates to reduced rates, and financial impacts, of identity fraud, improved confidence in administration and national security, and greater efficiency in border processing. Some of these benefits, and their additional costs, are difficult to quantify" (Auditor-General, 2008: 13).

In addition, full body scanning equipment has been introduced throughout Australian airports, but there are some concerns relating to privacy (Silmalis, 2012). For example, a former model and actress claimed she was singled out on a US internal flight and saw the Transportation Administration (TSA) officials "leering" at the sight of her full-body scan (Barlass, 2011). In May 2013 it was reported that the TSA had replaced the original scanners in favour of those showing only "generic images" of the body (Fox News, 2013). In Australia, a businessman and the leader of the United Australia Party, Mr Clive Palmer, stated in July 2013 that such scanners were "highly invasive" and, if elected, he would ban them (Feeney, 2013). There is also an issue of what to do about

passengers who refuse to undertake the full body scan and the religious and cultural factors.

Also on the subject of transport, routinely, cameras are installed in taxis to record the faces of passengers, ostensibly for crime prevention purposes and specifically to prevent persons absconding without paying the fare. Research has shown in Perth (Mayhew, 2000), and USA (Smith, 2005) that cameras in taxis do reduce crime. Although under the umbrella of publicly-accountable bodies, the examples of data collection cited above are almost entirely managed on a day-to-day basis by private organisations fulfilling outsourced contracts for government departments. Several cases of personal harassment or embarrassment relating to the privacy of citizens have been identified and there is also a question over what is done with the data after the citizen exits the means of transport. The next issue under discussion relating to privacy is intrusion into private communications.

INTRUSION INTO PRIVATE COMMUNICATIONS

Although in Australia there are strict laws (*Telecommunications (Interception and Access) Act 1979*) which have recently been strengthened relating to interception and access to telecommunications, there have been a number of concerns (e.g. Australian Government, n.d.; Bronitt & Stellios, 2006; Bronitt, Harfield, Michael, 2009; CJC, 1995; Grabosky, 1986; Grabosky, 1989; McGrath, 1990; Queensland Parliament, 2003; Stewart, 1986; Victorian Privacy Commissioner, 2004) over the years relating to the gathering of intelligence by this means. This includes the statement in the Stewart Royal Commission (1986: 1) that there was evidence New South Wales Police had been illegally intercepting telephone calls for 20 years (Dorling, 2012). In Australia, there have been five major reports (*Barrett Review* (1994); *The Boucher Review* (1999); *Ford Review* (1999); *Sherman Review* (2003); *Blunn Review* (2005)) dealing with telecommunications interception. Bronitt and Stellios (2006: 414) found legislators described that the overhaul of the legislation was "an exercise in 'balancing' the interests of privacy against the interests of security and law enforcement."

That was despite the New South Wales Law Reform Commission (NSWLRC, 2001: paragraph 24) concluding (in 2001) that the balancing approach was "inherently flawed." The Blunn Report (2005: 10) examined telephone interception and found there was a need for, "comprehensive and over-

riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established"; which led to the *Telecommunications (Interception and Access) Amendment Act 2007*.

The then Attorney-General described the 2006 legislation amendments as "enhanc[ing] interception powers and privacy protection" (Ruddock, 2006), but Bronitt & Stellios (2006: 424) concluded "While the reforms do enhance interception powers, we believe that these measures do not, to any *significant* degree, enhance privacy protections" (emphasis by original authors). The current law subject to various exemptions, states that a person shall not intercept, authorise, suffer or permit another person to intercept a communication passing over a telecommunications system. Time will tell if that updated law is effective in safeguarding privacy.

There have been a large number of enquiries and considerable public and political concern about "hacking" of mobile telephones in the UK following the investigation into illegal activities of reporters mainly from the *News of the World* newspaper which was owned by businessman, (Keith) Rupert Murdoch, AC, KSG. The full details and effects of what has been reported as disgraceful events were presented at the Canberra symposium on 8 August 2013 where this paper was presented (Beckley, 2013). The Leveson Inquiry (2012) interviewed 337 witnesses and found that newspaper reporters and operatives acquired 4,375 names and phone numbers of private citizens which involved 829 victims of mobile phone hacking. The Inquiry recommended a "genuinely independent and effective system of self-regulation" (Leveson, 2012: 13) but the UK Government is still considering this suggestion (i.e. at the time of this writing).

There is also concern about the development of "location based people tracking" (Michael & Clarke, n.d.) where mobile telephones with internal GPS (global positioning systems) tracking devices enabling satellite navigation also allow the individual mobile phone to be tracked within an accuracy of within a few metres, using triangulation methods. Researchers (Michael & Clarke, n.d.; Michael & Michael, 2009) describe location based people tracking as "uberveillance" which enables mobile phone companies to track customers so that commercial information and personal data can be extracted and fed into customer relationship management databases (Techtime, 2012).

Some of the outcomes of this tracking are undesirable (Haggerty & Samatas, 2010: 111–126 & 231–236; Neely & Barrows, 2012). Michael &

Michael (2009) found that data can be used to construct behavioural profiling and link owners to financial transactions and they warn of possible future "dystopian" scenarios in society. In addition, "Location-Based Social Networking" (LBSN) allows a member of a social network (e.g. Google Latitude, Loopt and BrightKite) to contact a "friend" remotely using a mobile telephone or other devices. This location information can be shared by persons known to the user or strangers and the service providers (Fusco, et al., n.d.). This issue links to the relatively recent phenomenon of social media.

Social Media

There is almost universal use of mobile phones, and Arthur (2012) explains that *Apps* on every smartphone are sharing data and uploading the phone owner's private contacts to the phone or social networking company (Facebook, Instagram, Yelp among others) but the phone user may be unaware that it is happening (Sarno, 2012). Mobile telephone users do not check the conditions of use provided with Apps that allow this data exchange to occur. Social media has achieved some good outcomes such as the so-called *Arab Uprising* that resulted in the overthrow of the Libyan dictator, Colonel Gaddafi; and the cause of *Kony 2012* (a major social media campaign organized by NGO *Invisible Children).* But, social media is also perceived negatively when used as a dynamic messaging device in incidents such as the street riots in the UK in 2011 (eBriefs, 2012).

There should be a great deal of concern over privacy issues relating to private communications and social media. It appears that citizens of the world are acquiescing to the ability of multi-national and trans-national private organisations collecting detailed personal and private data about their whereabouts, their needs and preferences and their financial status and spending. It also appears that technical experts can access private communications on mobile phones at will, again with little or no accountability. This critical discussion now turns its attention to DNA forensic strategies which in the UK were aimed at increasing the police detection rate by, "...deploying new technology, including enhanced DNA testing ... across the country to target criminals more effectively" (Home Office, 2004: 10).

DNA FORENSIC SAMPLES

In the UK, between 1 April 2011 and 30 September 2011 the National DNA Database produced 62 matches to murder, 285 to rapes and 15,685 to other crime

scenes (NPIA, 2011). The DNA databank in the UK in 2011 contained over 9 million records, which is one of the largest in the world and is a high proportion of the total population. However, researchers into crime detection statistics and the theory of *intelligence-led policing* (Ratcliffe, 2003) conclude that only a small percentage of the population is responsible for the majority of the crime (Audit Commission, 1993) although the perpetrators still need to be found in the database. The indefinite retention policy relating to DNA samples collected in the UK was challenged and found to be overly-invasive by the European Court of Human Rights in 2004.

In Australia, there are three DNA databases for law enforcement purposes. It is reported (Francis, et al., 2012) that there are over 450,000 person profiles (samples taken from suspected and charged persons) and 180,000 crime profiles (evidence taken from the scene of the crime). In 2010, Australia signed up to exchange DNA data with INTERPOL which is an international policing organization with 190 member countries. A research project in the USA (Roth, 2010) outlined concerns about DNA technology that makes it difficult for defendants to challenge and there is a chance of: (i) false matches and/or (ii) true match but coincidental. There are examples of DNA material being obtained by police by a trick (*Fleming v The Queen*, [2009] NSWCCA 233) and a "DNA testing flaw" found in Victoria (Silvester, 2009) that rendered some convictions unsafe (Griffith & Roth, 2006).

Research by Goodman-Delahunty & Hewson (2010) also found that statistics of certainty of matching quoted in DNA cases are difficult to understand for juries and there is an assumption ("the CSI effect") of the infallibility of the identification process. Roth (2010: 1,135) identified several problem issues and clear mistakes in the UK and the USA emanating from the main two types of DNA testing: confirmatory and cold case. All of the above is complicated by the latest developments in familial matching of DNA samples, the accuracy of which is not yet accepted globally, but was recently vindicated in proving that the Boston strangler crimes, the killing of 11 victims between 1962 and 1964, was in fact committed by the main suspect (Sherwell, 2013).

Although most DNA samples in the criminal justice system are collected by accountable organisations, in fact, most of the analyses of the samples are carried out by private laboratories or organisations which might lack accountability and security safeguards. The concerns relating to DNA samples and databanks are that confidential data could be obtained by health agencies and

insurance agencies, along with growth of the databanks which are described as being operated with a risk-based approach (Campbell, 2011: 55). This could lead to discrimination or restriction of goods and services to specific citizens suspected of debilitating medical conditions. There is evidence that "third party trackers" obtain user data from enquirers on websites relating to mental and medical health (*Sydney Morning Herald*, 2013). Having listed various issues relating to the privacy of the individual in democratic countries, this critical discussion will now draw some findings and conclusions from the previously discussed evidence.

CONCLUSION

Most organisations in the business of collecting intelligence will operate with the objective of acting lawfully and ethically but effective accountability needs to be established as this does not appear to be in place. This discussion has highlighted the fact that an increasing amount of personal data is being collected by private and public sector organisations through a variety of means such as CCTV and personal communications. It is necessary to reflect on the overall situation regarding the speed and intensity of data collection, performed by private and public sector organisations, which is increasing daily at a bewildering rate and is heavily impacting on the privacy of the individual citizen.

Details of investigations and whistle-blower announcements have revealed concerning issues relating to accountability of organisations that should have enhanced scrutiny and monitored the activities of their staff. It is not sufficient for executive managers to say they did not know the detailed activities of their subordinates; active supervision is required to prevent over-zealous or clearly criminal behaviour. The need to collect data should be balanced against the perceived outcomes, for example most research indicates that CCTV has no effect on reducing crime and anti-social behaviour although it does produce societal benefits in a few specific cases.

In terms of personal communications, there is a revolution and expansion of social media formats which enables the ability to contact and make acquaintances easily but also allows the facility to track and monitor personal locations, opinions, needs and requirements, which raises concern for confidentiality in the future. International cases raise the apprehension that criminals or hackers can access personal messages and private information from

mobile phones at will, raising an argument for greater encryption of mobile communications.

This critical discussion raises a debate around assessing the risk to the intrusion of intelligence gathering by investigating agencies (from the public *and* private sectors) on members of the public (the citizens and consumers) and asks the question: do the ends justify the means? The question is based on the test to decide if an action to obtain intelligence is ethically sound by asking several stages of questions relating to the good of the eventual outcome. That is: whether the means used will work effectively; whether there is a less harmful alternative and finally if the means undermines some equal or more important value. The intelligence gathering operative and practitioner should also recognise the risks relating to the justification of infringing human rights for the purpose of obtaining intelligence. A risk assessment should be carried out to establish the likelihood of harm occurring and the level of seriousness of the impact on the individual of the collection of intelligence (Beckley, 2012: 259); only where the risk is justified should the operation proceed.

The conclusion from this discussion must be that stronger scrutiny and safeguards are required to protect the privacy of the citizen in democratic societies. Judging by the comments of advice from the Federal Privacy Commissioner quoted above, it appears that individuals entrusted with guarding privacy have not been given adequate powers to enforce compliance.

Perhaps it is time for Australia to consider the introduction of the post of Surveillance Camera Commissioner (SSC) such as that in the UK. The SSC, who was appointed under the Protection of Freedom Act 2012, is about to issue new guidelines on surveillance cameras and ANPR (UK, 2013). Gathering all the evidence together about the daily erosion of personal privacy and confidentiality it is clearly time to take effective action to address these issues. On the positive side of the privacy equation, organisations responsible for gathering intelligence set a good example if, on every occasion, they are truly able to justify the resulting intrusions on the privacy of the individual citizen and retain dignity and justice for all of us which was the stated purpose of the *Universal Declaration of Human Rights* (UN, 1948).

REFERENCES

Anderson, J., & McAtamney, A. (2011). "Considering local context when evaluating a closed circuit television system in public places." *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology.

Arnold, B. (2008). "Privacy guide: CCTV & other cams." *Caslon*, Retrieved 14/02/2012, from www.caslon.au

Arthur, C. (2012, March 3). "Nothing sacred in online grab for data." *The Age*.

Audit Commission. (1993) *Helping with enquiries: tackling crime effectively*. London: HMSO

Auditor-General, The. (2008) *DIAC's management of the introduction of biometric technologies.* Audit Report No.24 2007–8 Performance Audit. Canberra: Australian National Audit Office.

Australian Customs Service. (2000) *Intelligence doctrine*, Canberra: Author.

Australian Government. (n.d.) 73—Other telecommunications privacy issues—interception and access. *ALRC.* http://www.alrc.gov.au/publications/73.%20Other%20Telecommunications%20Privacy%20Issues/interception-and-access

Australian Institute of Criminology. (2009). Using CCTV to reduce antisocial behaviour. *AICrime Reduction Matters.* Canberra: Author.

Ayuso, M., Guillen, M., Alcaniz, M. (2009) The impact of traffic violations on the estimated cost of traffic accidents with victims. *Accident Analysis and Prevention* 42 (2010) 709-717

Barlass, T. (2011, March 27). G-rated scanners for travellers. *The Sydney Morning Herald*.

BBC News (2009, December 19) *Councils 'treble CCTV in decade'*. Retrieved from: http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/8419358.stm

Beckley, A. (2000) *Human rights: the pocket guide.* London: The New Police Bookshop.

Beckley, A. (2002). The future of privacy in law enforcement or how Michael Douglas helped frame the law. *Society of Police Futurists International*: http://www.policefuturists.org/

Beckley, A. (2012) Capacity building, chapter 8. In: Aepli, P. (Ed.) *Toolkit on police integrity*. Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Beckley, A. (2013) *Intelligence: a risk too far or "dignity and justice for all of us?*" Conference presentation: *A symposium on the privatisation of intelligence* 08/08/2013, The National Press Club, 16 National Circuit Barton, Canberra. ARC Centre for Excellence in Policing and Security.

Bennett, T., & Gelsthorpe, E. (1998) Public attitudes towards CCTV in public places, studies in crime prevention. In Norris, C., Moran, J., Armstrong, G. (Eds.) *Surveillance, CCTV and Social Control*, Aldershot: Ashgate.

Bloss, W. P. (2009). Transforming US police surveillance in a new privacy paradigm. *Police Practice and Research: An International Journal*, 10 (3), 225–238.

Blunn, A. (2005). *Report of the review of the regulation of access to communications*. Canberra: Australian Government.

Bronitt, S., & Stellios, J. (2006) Regulating telecommunications interception and access in the twenty-first century: technological evolution or legal revolution? *Prometheus* 24:4, 413–428

Bronitt, S., Harfield, C., Michael, K., (Eds.) (2009). *The social implications of covert policing*. Wollongong: University of Wollongong Press.

Brooks, D., & Corkhill, J. (2012). The many languages of CCTV. *Australian Security Magazine*. Feb/March 2012: 57–59. Morley: My Security Media Pty Ltd.

Cameron, I. (2011) The cost of seeing clearly. *Policing Today*, 15.5, pp. 31–33.

Campbell, L. (2011) 'Non-conviction' DNA databases and criminal justice: a comparative analysis. *Journal of Commonwealth Criminal Law*, Issue 1, May 2011, pp.55–77

Carnovale, M. (2011). The face of crime. *Police Life*. April 2011, 28–29. Melbourne: Victoria Police Service.

Clarke, R. (2009) The covert implementation of mass vehicle surveillance in Australia. Chapter 6: pp. 47–62. In: Bronitt, S., Harfield, C., Michael, K. (Eds.) (2009) *The social implications of covert policing*. Wollongong: University of Wollongong Press.

Criminal Justice Commission. (1995). *Telecommunications interception and criminal investigation in Queensland.* Report 42. Brisbane: Author.

Cubbage, C. (2012). Public CCTV surveillance: networks & awareness. *Australian Security Magazine*. February/ March 2012: 56–57. Morley: My Security Media Pty. Ltd

Department of the Prime Minister and Cabinet (n.d.) Counter-terrorism white critical discussion: securing Australia protecting our community. *DPMC.* Retrieved from: http://www.dpmc.gov.au/publications/counter_terrorism/5_protection.cfm

Ditton, J. (1998) Public support for town centre CCTV schemes – myth or reality? In Norris, C., Moran, J., Armstrong, G. (Eds.) (1998) *Surveillance, CCTV and social control*, Aldershot: Ashgate

Dorling, P. (2012, February 18). Police spy on web, phone usage with no warrants. *The Sydney Morning Herald*.

Dorling, P. (2013, August 2) Spy program tracks "nearly all" web use. *The Age*: Retrieved from: http://www.theage.com.au/technology/technology-news/spy-program-tracks-nearly-all-web-use-20130801-2r2dc.html

Dowsley, A., & Flower, W. (2012, September 23) CCTV shows man in a blue hoodie spoke to missing ABC worker Jill Meagher moments before she disappeared. *Herald Sun*. Retrieved from: http://www.heraldsun.com.au/news/true-crime-scene/missing-woman-jill-meagher-seen-on-cctv-speaking-to-man-in-blue-hoodie-before-vanishing/story-fnat7jnn-1226479708333

eBriefs (2012, August 11) Police Superintendents Association of England and Wales: Cameron makes a statement of public disorder. House of Commons Main Statement. *UK Policing.* Retrieved from www.ukpolicing.info

Feeney, K. (2013, July 12) Palmer vows to ban body scanners after airport dispute. *Brisbane Times*. Retrieved from: http://www.brisbanetimes.com.au/queensland/palmer-vows-to-ban-body-scanners-after-airport-dispute-20130712-2pur0.html

Fox News, (2013, May 31) TSA gets rid of full-body scanners at US airports. Retrieved from: http://www.foxnews.com/politics/2013/05/31/tsa-gets-rid-full-body-image-scanners-at-us-airports/

Francis, B., Walsh, S., Hitchin, S. (2012) Australia signs on to the INTERPOL database. *Australian Police Journal,* March 2012, pp. 24–27

Fusco, S. J., Michael, K., Aloudat, A., Abbas, R., (n.d.). *Monitoring people using location-based social networking and its negative impact on trust*. Wollongong: University of Wollongong, School of Information Systems and Technology.

Gallagher, R. (2013, August 9) NSA spying on citizens' web activity "good news," ex-chief says. *The Sydney Morning Herald*

Gans, J., Henning, T., Hunter, J., Warner, K. (2011) *Criminal process and human rights*. Sydney: The Federation Press

Goodman-Delahunty, J. & Hewson, L. (2010) *Improving jury understanding and use of expert DNA evidence*. AIC Reports, technical and background Paper 37. Canberra: Australian Institute of Criminology.

Goold, B. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In: Schartum, D. W. (Ed.) *Surveillance in a constitutional government*. Social Science Research Network: 38–48.

Grabosky, P. (Ed.) (1986) *Government illegality*. Canberra: Australian Institute of Criminology

Grabosky, P. N. (1989). *Chapter 3: Telephone tapping by the New South Wales Police. Wayward governance: illegality and its control in the public sector.* Canberra: Australian Institute of Criminology: 47–65.

Griffith, G., & Roth, L. (2006) *DNA evidence, wrongful convictions and wrongful acquittals*. Briefing Paper No 11/06. Sydney: NSW Parliamentary Library Research Service.

Guardian, The. (2012, November 30) David Cameron statement in response to the Leveson Inquiry report. *The Guardian.* Retrieved from: http://www.guardian.co.uk/media/2012/nov/29/leveson-inquiry-david-cameron-statement

Haggerty, K. D., & Samatas, M. (Eds.) (2010). *Surveillance and democracy*. Oxford: Routledge.

Home Office (2004) *Cutting crime, delivering justice*, Cm 6288. London: HMSO

Kleinig, J., Mameli, P., Miller, S., Salane, D., Schwartz, A. (2011) *Security and privacy: global standards for ethical identity management in contemporary liberal democratic states*. Canberra: The Australian National University.

Lawson, S. D. (1991) *Red-light running: accidents and surveillance cameras*. Birmingham: AA Foundation for Road Safety Research and Birmingham City Council.

Leveson, B. (2012) *An inquiry into the culture, practice and ethics of the press*. The Leveson Inquiry. Executive Summary. November 2012. HC779. London: The Stationery Office.

Mayhew, C. (2000) Preventing assaults on taxi drivers in Australia. No. 179, November 2000. *Trends and issues in crime and criminal justice.* Canberra: Australian Institute of Criminology.

McCahill, M., & Norris, C. (2012) *CCTV in London*, Working Critical discussion No.6. Berlin: Urbaneye

McDevitt. B. (2010, October) *Automatic number plate recognition systems*. Presentation at *International and Serious Organised Crime Conference.* 18–19 October 2010, Melbourne: Australian Institute of Criminology.

McGeough, P. (2013, July 20) Manning may spend life in jail as judge upholds crucial charge *The Sydney Morning Herald*, p14

McGeough, P. (2013, August 1) Pyrrhic victory seals leaker's fate. *The Sydney Morning Herald*

McGrath, G. M. (1990) *Telephone interception: watching brief report*. Sydney: National Police Research Unit.

Michael, K., & Clarke, R. (n.d.) *Location privacy under dire threat as uberveillance stalks the streets*. Wollongong: University of Wollongong

Michael, M. G., & Michael, K. (2009). *The fall-out from emerging technologies: on matters of surveillance, social networks and suicide.* Wollongong: University of Wollongong.

National Policing Improvement Agency. (2011) *DNA technology crime detection*. Retrieved from: http://www.npia.police.uk/en/8934.htm

National Policing Improvement Agency. (2012) *Automatic number plate recognition*. Retrieved 2012, February 14 from: http://www.npia.police.uk/

Neely, A., & Barrows, E. (2012). *Are you giving away your most intimate secrets when you shop? See how Target learns about you through the power of analytics*. Retrieved 2012, March 8 from: www.cambridgeperformancepartners.com/blog/2012/2/19/are-you-giving-away-your-most-intimate-secrets-when-you-shop.html

New South Wales Law Review Committee (2001) *Surveillance: an interim report*. No 98, 2001. Sydney: NSW Government.

OFPC (2008) *Inquiry into automatic number plate recognition technology submission to the Queensland Parliamentary Travelsafe Committee*: Issues Critical discussion No. 12. Office of the Federal Privacy Commissioner, February 2008. Retrieved from: http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/inquiry/ANPR%20technology/Submissions/28.pdf

Pointing, B. S. (2012) Effective use of CCTV camera operators. Perth: *Australian Security Magazine*, February/March 2012

Porter, G. (2009) CCTV images as evidence. *Australian Journal of Forensic Sciences*, 41:1, 11–25

Queensland Parliament. (2003) *"Telephone tapping" powers for Queensland law enforcement agencies: the Telecommunications (Interception) Queensland Bill 2003 (Qld)*. Brisbane: Queensland Parliament.

Ratcliffe, J. H. (2003) Intelligence-led policing. *Trends & issues in crime and criminal justice* April 2003, No.248. Canberra: Australian Institute of Criminology.

Roth, A. (2010) Safety in Numbers? Deciding when DNA alone is enough to convict. *New York University Law Review*, vol 85: 1130.

Risen, J. (2013, July 9) Privacy lobby challenges NSA spying in highest court. *The Sydney Morning Herald*

Ruddock, P. (2006, March 30) *Enhanced interception powers and privacy protections*, Press Release, 30 March 2006. Sydney: NSW Government

Sarno, D. (2012, February 17). Smartphones exposed to new data mining. *The Sydney Morning Herald*.

Scott, S. L. (n.d.) Death of James Bulger. *Trutv*. Retrieved from: http://www.trutv.com/library/crime/notorious_murders/young/bulger/1.html

Sherwell, P. (2013, July 13) DNA sparks breakthrough in Boston Strangler case. *The Sydney Morning Herald*

Silmalis, L. (2012, February 5). Full-body scans rolled out at all Australian international airports after trial. *The Sunday Mail*.

Silvester, J. (2009, December 10) New DNA testing flaw. *The Age*. Retrieved from: http://www.theage.com/national/new-dna-testing-flaw-20091209-kk22.html

Silvester, J., & Butt, C. (2012, September 28) Man arrested over Jill Meagher case. *The Sydney Morning Herald*. Retrieved from: http://www.smh.com.au/victoria/man-arrested-over-jill-meagher-case-20120927-26nu7.html

Smith, M. J. (2005) *Robbery of taxi drivers. Problem-oriented guides for police.* Problem-Specific Guides Series No. 34. Washington DC: US Department of Justice. Office of Community Oriented Policing Services.

Stewart, D. (1986) *Royal Commission into alleged telephone interceptions*. April 1986. Sydney: NSW Government

Sutton, A., & Wilson, D. (2004) Open-street CCTV in Australia: The politics of resistance and expansion. *Surveillance and Society* 2(2/3): 310–322.

Sydney Morning Herald, The. (2013, July 10) Health privacy now in the eye of the spy. *The Sydney Morning Herald.*

Techtime. (2012) Futuristic facial detection and tracking technologies help retailers analyse store performance. *Australian Security Magazine*. December 2011/January 2012. Morley: My Security Media Pty. Ltd.

UK Government. (2013) *Surveillance Camera Commissioner*. Retrieved from: https://www.gov.uk/government/organisations/surveillance-camera-commissioner

United Nations. (1948) *Universal declaration of human rights*. Geneva: UN.

Victorian Privacy Commissioner (2004) *Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee on its inquiry into the provisions of the Surveillance Devices Bill 2004*. (23 April 2004).

Victoria: Government Printers.

Watson, B., & Walsh, K. (2008) *The road safety implications of automatic number plate recognition technology*. Brisbane: The Centre for Accident Research & Road Safety.

Welsh, B. P., & Farrington, D. C. (2008). Effects of closed circuit television surveillance on crime. *Campbell Systematic Reviews*, 2008:17, Retrieved 2013, May 17 from: http://www.campbellcollaboration.org/

Western Australia Auditor General. (2011) *Use of CCTV equipment and information*. Western Australia Auditor General's Report. Perth: WAAG.

Wilson, D., & Sutton, A. (2003). Open-street CCTV in Australia. *Trends and issues in crime and criminal justice* (271). Canberra: Australian Institute of Criminology.

ABOUT THE AUTHOR

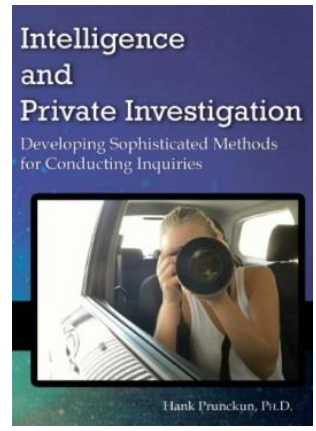
Alan Beckley is Evaluation Manager and Adjunct Research Fellow at University of Western Sydney. He is an Associate Investigator with the Australia Centre of Excellence in Policing and Security (CEPS) and was a graduate of FBI National Academy while he was a serving police officer in the United Kingdom. Beckley is currently completing a PhD on Human Rights and Ethical Standards in Policing.

- o O o -

Book Review

Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries

by Hank Prunckun, editor
Charles C. Thomas Publisher, Ltd., Springfield, IL.
2013, 220 pages, illus., tables, index
ISBN 978-0-398-08888-0



Reviewed by Robert Bostelman
Insight Intelligence, Sydney

Whether you are an experienced investigator, someone new to the field, or a person thinking of entering the field *Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries*, edited by Dr Hank Prunckun, challenges the reader not only to look within in an attempt to curb preconceived views or biases, but to look at the field of investigation in an entirely new light.

This book shows how rapidly private investigation and intelligence is evolving, but also how it is promoting a "revolution" in the field. In my view, this book challenges experienced investigators to evolve and take a more holistic view of the field of investigation; moving inquiry agents into intelligence-based investigations. As a new investigator, or someone looking to build a career in this field, this book provides some exciting insights into how multi-faceted the field of intelligence and private investigation actually is, and the fascinating options available to the modern day investigator.

Intelligence-led investigations is a new approach in the private investigations field that inspires investigators to adopt a range of analytical methods that add to general factual based investigations. Within the policing field, intelligence-led investigations focus on interpreting criminal activity. For private investigators there also exists an opportunity to develop interpretative skills when approaching factual and surveillance cases. For example, this book highlights the role of an analysis of competing hypotheses. Through this approach the investigator is able to begin moving from simply providing facts to

providing analysis of events and circumstances. Essentially, competing hypotheses is about brainstorming a range of possibilities in a given situation and making an argument for-or-against each of the possible hypotheses. While perhaps common place amongst government intelligence agencies, such an approach could propel private investigations into a more sophisticated form of inquiry.

This book's strength is its ability to illustrate how the field—particularly in the last ten years—has evolved and how some of the techniques formerly used by military or national security analysts can be integrated into intelligence-based investigations in the private sector. Further, with the growth of social media and other open-sources of information this book discusses how such information can be gathered and used in intelligence-based investigations (by Jeff Corkill, Edith Cowan University). This is discussed within the legal and ethical constraints that PIs operate, and are covered in dedicated chapters by Professor Rick Sarre and former-Detective Chief Superintendent Mark S. Bradley, respectively.

With claimants and respondents rapidly becoming more sophisticated, and clients becoming better informed, there is a greater demand on the modern day investigator. Clients not only require factual information, they demand answers; sometimes to multiple hypotheses during the course of an investigation, so this book provides both practical and theoretical knowledge as well as solutions for addressing these dilemmas. This bodes well for PIs because it assists them navigate through the "operational minefield" towards better investigative outcomes.

In essence, this book provides social and historical context for the field of investigation and how today's investigators need to have a greater understanding of a very diverse society made up of a multitude of cultures and influences. This in turn allows for a greater understanding and better interaction with people and organisations in general. The book takes the reader through numerous intelligence-based topics, including target profiling (Tony Buffett, Charles Sturt University), fraud intelligence (Rebecca Vogel, Macquarie University), political intelligence (Dr Troy Whitford), anti-terrorist and anti-gang intelligence (Dr Hank Prunckun), illicit organisations and financial intelligence (Levi J. West, Charles Sturt University), counterintelligence (Dr Petrus Duvenage), and covert communications (military intelligence specialist, Michael Chesbro), but in doing so explains how these fields overlap. These chapters may also provoke a passion for a more specific career and gives the budding investigator food for thought in regards to where private investigation could take them. Of particular note are the

contributions made by Dr Patrick F. Walsh who wrote on investigative intelligence and Dr Troy Whitford who called for investigators to develop a practice of lifelong learning.

Overall, Dr Prunckun has assembled a number of experts in the field (four were also government licenced PIs) and should be commended for his ability to shape such a diverse collection of perspectives into a readable examination of a topic that has been crying-out for greater professionalisation. He was able to bring private investigations into the Twenty-First Century illustrating the commonalities, or perhaps the positive influences, national security and law enforcement agencies can have on the industry.

The book engages its reader through the variety of interesting exercises and self-reflection activities that capitalises on the existing practices of the private investigator, and serves as an educative self-study guide. This book is able to provide strategies on how to grow and become a well-rounded investigator through providing mechanisms to expand their skillset and discard some of the preconceived ideas of private investigations and what it actually means to be a modern day investigator.

Having worked in the private investigation industry for many years, both in the field and in a management and consultative capacity, I recommend the book to investigators, educators, and investigation agencies alike. It is an interesting read with contributions from experts from the "five eyes" intelligence alliance. This is a book that will no doubt be used as a resource in intelligence and private investigation fields for many years to come.

ABOUT THE REVIEWER

Robert Bostelman, BA(Psy), holds a Certificate III in Investigative Services and has extensive experience as a licenced PI encompassing the information technology, insurance, and other investigative industries spanning a twenty year career. He is a highly-skilled fraud investigator with well-developed intelligence gathering, analytic, and inquiry skills. He has worked for many large private entities, major insurers, solicitors, and investigation providers involving all fields of fraud. Mr Bostelman now manages the national operations of Insight Intelligence, a national firm that provides investigator training, quality assurance, and facilitates workshops on topics such as profiling and questioning techniques. Insight Intelligence has a range of large private entities and major insurers as its clients.

Call for Papers

Salus Journal is a peer-reviewed open access e-journal for the publication of law enforcement and security agencies, as well as research findings and discussion papers regarding emergency management and public safety. *Salus Journal* seeks to contribute to practice by inspiring discussion through an interdisciplinary approach.

We invite submissions of articles of between 3,000 and 6,000 words for double-blind peer review that:

- focus on issues that have an impact on criminal justice, law enforcement, national security, or emergency management;
- engage with contemporary topical practice issues; or
- add to the understanding of complex management conundrums.

Submissions can use either qualitative or quantitative approaches, including studies that employ the use of exploratory or holistic approaches. The journal also accepts discussion papers, or essays, as long as a clear position is stated and the argument is grounded in sound practice, or the subject literature.

Book Reviews

Salus Journal also accepts book reviews that do not exceed 750 words. Reviews should go beyond the descriptive account of the book's contents. Reviews that discuss the implications of the book's message for practice or policy are sought for inclusion in future editions. Books can be either newly published, or vintage editions where the book's thesis can be applied to a current situation or in newly emerging context.

Submission Process

Visit the journal's submissions page to see a copy of the author guidelines and a summary of the refereeing process:

www.salusjournal.com/submissions