Australia and the New Technologies: Evidence Based Policy in Public Administration

Editors: Katina Michael and M.G. Michael

RNSA

Research Network
Secure Australia

The Third Workshop on the Social Implications of National Security

Australia and the New Technologies: Evidence Based Policy in Public Administration

23-24 July 2008
Canberra, Australia

Editors: Katina Michael and M.G. Michael

Research Network for a Secure Australia

This event is organised by the Research Network for a Secure Australia (RNSA). RNSA is a multi-disciplinary collaboration established to strengthen Australia's research capacity for protecting critical infrastructure (CIP) from natural or human caused disasters including terrorist acts. The RNSA facilitates a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues relating to critical infrastructure. World-leaders with extensive national and international linkages in relevant scientific, engineering and technological research will lead this collaboration. The RNSA also organises various activities to foster research collaboration and nurture young investigators.

Participants are encouraged to join the RNSA. Membership of the RNSA is open to Australian and international researchers, industry, government and others professionally involved in CIP Research. Information on joining is at www.secureaustralia.org.

RNSA

Convenor:	A/Prof Priyan Mendis, Head of the Advanced Protective Technology for Engineering Structures Group at the University of Melbourne
Node Leader:	Prof Joseph Lai, UNSW@ADFA
Node Leader:	Prof Ed Dawson, Queensland University of Technology
Node Leader:	Prof Hussein Abbass, UNSW@ADFA
Research Program Manager:	Dr Tuan Ngo, University of Melbourne
Administrative Support:	Mr Anant Gupta, University of Melbourne
Outreach Manager:	Mr Athol Yates

University of Wollongong

Editors: Michael, K. and Michael, M.G.
Publication Title: Australia and the New Technologies: Evidence Based Policy in Public Administration (Workshop on the Social Implications of National Security, 2008)
Series: Research Network for a Secure Australia (RNSA)

Publisher: University of Wollongong,
IP Location-Based Services Research Program (Faculty of Informatics)
Contact Details: Tel 02 4221 3937, Fax 02 4221 4045, University of Wollongong NSW 2522
Conference Websites: http://www.secureaustralia.org/ & http://www.uow.edu.au/~katina/rnsa08.htm
Publication Year: 2008
Format: Book (hardcopy $50 AUD; softcopy $30 AUD from http://www.homelandsecurity.org.au/publications.html)
Cover and text layout: Anthony Petre

ISBN: 978-1-74128-150-7 (print)
ISBN: 978-1-74128-151-4 (pdf)

Foreword

The 2008 Workshop on the *Social Implications of National Security: Australia and the New Technologies- Evidence Based Policy in Public Administration* was organised by the Research Network for a Secure Australia (RNSA) funded by the Australian Research Council. The Workshop is a biennial event bringing together both researchers and practitioners in the fields relating to the national research priority entitled Safeguarding Australia. In 2008, the workshop was held on the 23rd-24th July, at Hotel Realm in Canberra between 9.15 am and 3.30 pm.

The Workshop was organised by RNSA members from the IP Location-Based Services Research Program (Faculty of Informatics) from the University of Wollongong, jointly with the University of Melbourne and the Australian Homeland Security Research Centre.

This workshop addresses the application of evidence based policy in public administration. It specifically focuses on the issue of new technologies in the form of product and process innovations rolled out in Australia since major international events (e.g. Sept 11, Boxing Day Tsunami, Avian Flu outbreak). These product and process innovations introduced for the ‘common good’ are usually mandated by government agencies, designed and implemented by private business, and obligatorily adopted by citizens in the name of national security.

The workshop investigates how information is gathered, processed and disseminated to provide evidence toward policy making. What qualitative and quantitative methods are used to make public administration decisions; how stakeholders are engaged and brought into the wider debate; how legislation is introduced and its effect; what ethical considerations are made prior to implementation of mass market information technologies; and the importance of maintaining the rights of citizens.

The workshop brings together academics and practitioners from multiple disciplines including law, information technology, sociology, ethics, policy, medical, business, accounting and economics.

The workshop included papers by Professor of Medicine Chris Del Mar (keynote), Associate Professor of Counter-Terrorism Nicholas O’Brien, Professor of Transport Systems Marcus Wigan, Executive Director of Cyberspace Law and Policy Centre David Vaile, Professor of Social Planning

Rob Watts. Other professionals presenting included Professor Roger Clarke Principal of Xamax Consultancy, Mr Rob Nicholls and Ms Michelle Rowland with Gilbert + Tobin, Dr Lucy Resnyansky a research scientist with the Defence Science and Technology Office, Mr Mark Loves of the Centre for Transnational Crime Prevention, Mr Nigel Phair Principal of eSecurity Consulting, and Ms Suzanne Lockhart CEO of Biometric Consulting Group.

The Workshop Proceedings contain both peer reviewed papers and extended abstracts. The acceptance rate was 73%. Peer reviewed papers are identified with an asterisk in the contents page.

The editors would like to thank all of the reviewers for their assistance in maintaining the high quality of papers, which are indicative of cutting-edge research in the field. A special thank you also to the authors of these proceedings, who dedicated so much of their time to support the workshop, especially for the time dedicated to researching and writing up the results of their individual projects.

Program Committee

With respect to the organisation of the 3rd *Social Implications of National Security* workshop, the Chair received feedback from the following RNSA members.

Associate Professor Priyan Mendis
Mr Athol Yates

We would also like to acknowledge the support of the Dean of the Faculty of Informatics Professor Joe Chicharo, and the Head of the School of Information Systems and Technology Associate Professor Peter Hyland of the University of Wollongong.

Workshop Committee

Chair and Editor: Dr Katina Michael
Co-Editor: Dr MG Michael
Co-Chair: Dr Holly Tootell

Reviewers

The editors would like to thank the following reviewers for their assistance.

Dr Glenn Bewsell	*Lecturer, Faculty of Informatics, University of Wollongong*
Professor Simon Bronitt	*ANU College of Law, Australian National University*
Mr Mark Burdon	*Research Associate, Queensland University of Technology*
Professor Joan Cooper	*Pro-Vice Chancellor (Students) & Registrar, University of New South Wales*
Mr Luke Howie	*Lecturer, Faculty of Arts, Monash University*
Associate Professor Peter Hyland	*Head of School of Information Systems and Technology University of Wollongong*
Professor Margaret Jackson	*School of Accounting and Law, RMIT University*
Mr Murray Long	*Murry Long and Associates*
Professor Brian Martin	*Faculty of Arts, University of Wollongong*
Mr Glen Mattocks	*Visor Consulting*
Dr Lauren May	*Senior Lecturer, Queensland University of Technology*
Ms Nicola McGarrity	*Research Associate, Gilbert + Tobin Centre of Public Law, University of New South Wales*
Dr Katina Michael	*Senior Lecturer, Faculty of Informatics, University of Wollongong*
Dr M.G. Michael	*Honorary Fellow, Faculty of Informatics, University of Wollongong*
Professor Bill Russell	*Deputy Head of GAMUT, University of Melbourne*
Associate Professor Jill Slay	*School of Electrical and Information Engineering, University of South Australia*
Dr Holly Tootell	*Lecturer, Faculty of Informatics, University of Wollongong*
Dr Ping Yu	*Senior Lecturer, Faculty of Informatics, University of Wollongong*

Table of Contents

Peer reviewed papers are identified with an asterisk.

1

Editorial: What is evidence-based policy (EBP)?

Katina Michael[1] and MG Michael[2]

[1]Senior Lecturer, School of Information Systems and Technology, University of Wollongong, [2]Honorary Fellow, School of Information Systems and Technology, University of Wollongong

Evidence-based policy (EBP) is an approach to decision-making in government which stipulates that policy-setting should be based on objective evidence. EBP is sometimes accompanied by the word "practice" or "praxis"[1] as in evidence based policy and practice (EBPP),[2] highlighting the importance of merging political ideals with social and technical research without excluding the all important factor of *practice* (i.e. experience from the field). EBP is widely used in the health sector, with reference to evidence-based medicine. For example, the *Cochrane Collaboration* of whom Professor Chris B. Del Mar (keynote address) is a member of was

> "established to ensure that up to date, accurate information about the effects of healthcare interventions is readily available worldwide. It produces and disseminates systematic reviews of healthcare interventions, and promotes the search for *evidence* in the form of trials and other studies of the effects of interventions…"[3]

EBP has also entered the rhetoric of the government sector, and today even social researchers who were once sceptical about the approach, engage collaboratively with the method.

Not surprisingly given the appeal of EBP to different sectors, the approach has

[1] Bev Rogers, 'Educational Research for Professional Practice: More Than Providing Evidence for Doing 'x Rather Than y' or Finding the 'Size of the Effect of A on B" (2003) 30(2) *The Australian Educational Researcher* 65.

[2] Sandra Nutley, Huw Davies and Isabel Walter, 'Evidence Based Policy and Practice: Cross Sector Lessons from the UK' (Paper presented at the Social Policy Research and Evaluation Conference, Wellington, New Zealand, 2-3 July 2003 2003).

[3] Chris Del Mar and Tom Jefferson, *Cochrane Collaboration* (2006) Bond University <http://www.bond.edu.au/cochranegroup/> at 9/06 2008.

been adopted and adapted by different stakeholders to suit accordingly. Nonetheless, the common emphasis is on *evidence*: applicatory knowledge that can be used to direct policy-makers to concentrate on fundamental issues affecting all civil society. It is more than 'agenda-setting,' it is an effort to address key issues, to prioritise principal areas of concern, and to construct and deliver solutions that serve the common good. The hope is that citizens will be better off., in a wide range of situations. The basic premise of EBP is that if quality information can be collected about a given issue and processed into more meaningful knowledge, and disseminated to stakeholders who have the power to act, that decisions about the public good can be made in a timely manner. Ideally this type of policy setting should be proactive in countering negative forces before they occur, and oppositely capitalizing on positive forces just-in-time. Risk models are now routinely devised across the government sector to help in assessing trade-offs between areas of concern. These models are intrinsically linked to rewards and losses and are introduced to help policy makers make their judgments. The whole point of this type of analysis is to conduct scientific studies that demonstrate that particular programs or practices can lead to better policy outcomes. As in the area of evidence-based medicine which is about proven methods that work to prevent disease, make the sick better, or completely cure an individual, evidence-based policy is about "what works"[4] for the State in terms of public administration.

How we prioritise what is most significant to a State can be derived in a number of ways. Traditionally it is about taking care of the masses by providing a good health system, housing affordability and educational requirements, i.e. basic human rights.[5] However, if we look at the domain of national security, policy has swayed depending on the global political climate at a given point in time. More recently terrorist strikes abroad that have impacted Australians have fuelled media attention and subsequently public opinion locally. The Australian government swiftly responded to terrorist attacks like the Bali Bombing, Jakarta Bombing, and strikes on other States as it was considered critical to do so. Often subjects like terrorism are perceived as requiring urgent attention by policy makers, ahead of other national matters because of the psychological effects they can have on a populace. It is quite possible that a government may rapidly respond to a mass casualty terrorist attack by enlisting the support of businesses specialising in information and communication technology (ICT) to develop anti-terrorism solutions in the hope that future onshore attacks will be prevented. In fact, this is partially why Australia's ePassport made its entry when it did, despite it not having undergone exhaustive testing. Other technologies that were considered for national deployment in Australia after 9/11 included the proposed Access Card scheme, advanced closed circuit television (CCTV), and location-based services (i.e. telecommunications interception).

[4] H. Roberts, 'What Works?' (2005) 24 *Social Policy Journal of New Zealand* 34.

[5] General Assembly of the United Nations, *Universal Declaration of Human Rights* (1948) <http://www.un.org/Overview/rights.html> at 13 July 2008.

One problem associated with these new technologies is that they have enjoyed limited public debate prior to implementation, and more importantly little has occurred in the form of educational awareness campaigns before deployment. Consider the ePassport for instance which was issued to new passport holders or citizens renewing their passports without warning or explanation. A message inside the passport simply read:

> "This passport contains sensitive electronics. For best performance, please do not bend, perforate or expose to extreme temperatures or excess moisture | This passport contains a contactless integrated circuit chip which is an electronic device. In addition to the normal care and respect afforded a passport, please regard this document as you would any other portable electronic device, by ensuring that it does not become wet, folded or mutilated. Abuse may adversely affect the operation of the chip and reduce its utility to the bearer and to the border inspection personnel."

No other detailed information accompanies the passport explaining how the device may be used by government personnel or indeed, what some of the risks to the citizen might be. Here Alvin Toffler's concept of *Future Shock*, "too much change in too short a period of time" comes to mind. The fundamental question here is how was the ePassport application proven in? On what basis or evidence did the Government at the time make their decision to introduce a passport that relied on the most insecure of automatic identification technologies, Radio Frequency Identification (RFID)?

In our attempt to *measure* and *evaluate* almost everything we seek to define or question, quantitative studies (e.g. randomized experiments) by default have become more acceptable than qualitative studies (e.g. histories). It is unfortunate that quantitative studies for the greater part are given more respect and attention by analysts, even when conducted poorly. Almost instinctively we will dedicate more time to a report that shows figures, negating the multiple levels of assumptions that may have crept into the business case or privacy impact assessment. We are generally obsessed with creating models that will tell us how to prioritise lists, right down to decimal point values; and on what indicator to sort by even if the ultimate figure is arbitrary. The latest modelling trend is to map value chains and to consider interdependencies in critical infrastructure in order to simulate 'what if' scenarios and 'how to' responses. It is not that these models are necessarily wrong or should not be developed, but we marginalize or neglect to consider other important qualitative factors that will give us a bigger and clearer picture of the way forward. Sometimes what is more telling is not what a business case has actually included in terms of global variables and formulae, but what it has failed to address and excluded. The classic financial indicator which is often considered significant for proving in a business case is return on investment (ROI)- but how does one begin to calculate ROI for an Access Card scheme that is said to combat terrorist threats? How does a figure calculated for a given snapshot in time address longer term social risks and implications for citizens? In short, it does not. This is especially true when there is no historical evidence to go by, and a new innovation, process, product or service is being introduced for the first time as a solution to a problem.

⋆

Governments today are interested in managerial models of *efficiency* and *effectiveness*,[6] stemming from innovation and competition, and answering the difficult questions often related to national budgets, strategic options and direction, program management, outcomes and evaluation (i.e. the notion of value for money). Before being elected into government, Kevin Rudd made it clear that he embraced EBP as an approach to policy setting, when he told ABC:

> "I'm a Labor moderniser. Always have been, always will be and what that's on about is good evidence based policy in terms of producing the best outcomes for this nation, carving out its future in a pretty uncertain century where things fundamentally are changing. The rise of China, the radical changes in the Asia Pacific region, the globalisation of the economy, great fundamental technological challenges like the digital revolution, the future of broadband, to be part and parcel of all that as a Labor moderniser, and to be serious about what I would describe as enabling our community through an education revolution. And through the proper provision of basic services like health and hospitals to be part and parcel of the country's future."[7]

Some might be critical and say that Rudd's style of government was opportunistic in an attempt to win points with citizens and stakeholders by increasing the perception that policy makers are 'listening' to every day Australians. Others might say that the government is indeed collaborating jointly with the community by involving them in the decision making process. The *2020 Summit*, held on the 19-20 April 2008 was one of these examples. The Summit was a classic network, bringing together business people, experts and community leaders alongside policy makers, trying to share in a common strategic vision of the nation's future on important issues of the economy, the nation's infrastructure, the environment, agriculture, health care, indigenous Australians, the arts, and national security.[8] EBP is particularly renowned for strengthening the customer-owner-provider relationship.

In one of his first speeches after his election, Prime Minister Rudd highlighted the development of contestable evidence-based policy making processes as one of the seven major elements of the Government's vision. He said:

> "The Government must receive the best advice, based on the best

[6] Brian Head, *Evidence-Based Policy* (2006) Australian Research Alliance for Children and Youth <www.jcipp.curtin.edu.au/local/docs/Paper-Head.PPN2006.ppt> at 29 May 2008.

[7] Tony Jones, 'Tony Jones talks to Opposition Leader Kevin Rudd' (2007).

[8] Australian Government, *Australia 2020 Summit* (2008) Australian Government <http://www.australia2020.gov.au/> at 5 June 2008.

> available information and evidence… policy design and policy evaluation should be driven by analysis of all the available options, and not by ideology… The Government will not adopt overseas models uncritically.We're interested in facts, not fads. But whether it's aged care, vocational education or disability services,Australian policy development should be informed by the best of overseas experience and analysis… It may be appropriate to collaborate with a State government, a business organisation, a research centre or a community organisation. It may even be appropriate to cooperate on policy innovation with a government agency overseas… Policy innovation and evidence-based policy making is at the heart of being a reformist government. Innovation can help us deliver better policy and better outcomes for the whole community."

Yet, EBP does not escape the age-old problem of what actually constitutes evidence? Is evidence *fact*, and can we really determine who is correct? Is evidence *truth*? What does it mean to have 'enough' proof? How sure can we be about what we are proposing based on data sets?[9] Does it matter who is premised with gathering the evidence and what their stake is in a given project? Are consultants who are engaged by government to carry out rigorous studies truly impartial? This is a sticking point for those working in the area of 'proving in' policies.

One recent government report on Australia's youth rightly stated that "[r] esponsible risk assessment seeks to ensure decision-making that is ethical, evidence-based and defensible." But perhaps it is all a matter of interpretation. *Ethics* is defined as "the philosophical study of morality, a rational examination into people's moral beliefs and behaviour."[10] The *Macquarie Dictionary* defines *morals* as being concerned with the distinction of right and wrong.[11] *Truth* plainly can be considered as *fact*, although the term extends to other notions including *honesty* and *reality* which can add a level of ambiguity to the definition.[12] For instance, whose reality is being considered and why? And what of the beliefs and religious or philosophical orientation of the individual providing the evidence? Is *truth* absolute or is *truth* relative?[13] One could even be so cynical as to claim that the questions themselves

[9] Brian Head, *Evidence-Based Policy* (2006) Australian Research Alliance for Children and Youth <www.jcipp.curtin.edu.au/local/docs/Paper-Head.PPN2006.ppt> at 29 May 2008.

[10] Michael J. Quinn, *Ethics for the Information Age* (2006) 55.

[11] 'Ethical Objectivism' in Ted Honderich (ed), *The Oxford Companion to Philosophy* (1995) 631. There is a range of views about moral judgments. "At the subjectivist pole, they are taken to be discrete feeling-responses of individuals to situations actual or imagined. To move towards the objectivist pole is to argue that moral judgments can be rationally defensible, true or false, that there are rational procedural tests for identifying morally impermissible actions, or that moral values exist independently of the feeling-states of individuals at particular times."

[12] Peter Vardy, *What is Truth?* (1999).

[13] 'Ethical Relativism' in Kenneth McLeish (ed), *Guide to Human Thought: Ideas that Shaped the World* (1993) 248. "Ethical relativism, in philosophy, is the view that ethical judgments are true or false only relative to a particular context."

we are posing, by their very nature, may be predisposed to ruling out particular types of evidence as irrelevant or ideological.

⋆

EBP at its core is certainly not new though in places it might be presented as such given our ever-increasing obsession with surplus 'innovation' at all levels of research. The Ancient Greeks (but also modern logical empiricists) understood 'hypothetico-deductive systems' as sets of laws bound together from a select set of propositions where all else necessarily follows as a deductive consequence. "Explanation therefore is a matter of showing how things will happen in accordance with the laws of the theory." However, as Michael Ruse critically points out (directing us to William Whewell's 'consilience of inductions') and something which we should all note is "the fact that really successful theories bind together information from many hitherto disparate areas of experience."[14]

This workshop endeavours to consider Australia and the manner in which new mass market information and communication technologies have been deployed in response to national security issues, recognising both the benefits and limitations of evidence based policy as an approach to policy setting. The workshop has global appeal in its outcomes.

[14] 'Theory' in Ted Honderich (ed), *The Oxford Companion to Philosophy* (1995) 871.

2

Using the tools of evidence-based practice in making decisions on national security

Chris Del Mar

Professor, Dean, Faculty Health Sciences and Medicine, Bond University

Abstract

Evidence-based practice (EBP) developed out of an imperative to adopt a greater empiricism in deciding what strategies are effective in caring for patients. This supplements the previous emphasis on the 'scientific' understanding disease, diagnosis and treatment processes. Its results have been often startling. Much of what we had been doing clinically was useless, and what we had not been doing was useful. The fact that EBP allows a quantification of effect has provided much better estimates of effectiveness than in the past. Using a recent review of physical barriers to prevent infections from virus infections, something of immediate application to national security, some principles of EBP are outlined. These principles can be used for decision-making in many areas, including national security.

Keywords: Evidence, evidence-based practice, evidence-based policy, decision-making

1 Introduction

Evidence-based practice (EBP) arose out of McMaster University in Canada in response to the introduction of a new very short medical program (three years). It was clear that traditional teaching was untenable, and students would have to learn to find information rather than simply learn it. That this would be good preparation for maintaining currency was a benefit too. But deciding what systems were needed to estimate the quality of the information was necessary. These systems, and others needed to complete the process were called "Evidence-Based Medicine", a term coined by a physician, David Sackett.[1]

The movement was found effective in medical education. It quickly spread to post-graduate medical education, as well, and thence to continuing medical education. From there it became embedded in clinical practice world-wide, and spread into other clinical areas, when it was known as EBP. It has extended into health policy (Evidence-Based Health Policy) and into policy more generally (Evidence-Based Policy).

2 What is evidence-based practice?

EBP is a method of establishing clinical questions, formatting them in a way amenable to being answered, searching for evidence, making a decision about the quality of that evidence, and then applying to the setting from which the question arose initially. This can be summarised as the "4-As":

- Asking;
- Accessing;
- Appraising;
- Applying.

'Evidence' is used very specifically to mean 'empirical evidence', that is, evidence that is not dependent on understanding the mechanism of disease or its clinical management (understanding that has been flawed on occasion, and leading to inappropriate clinical managements), but simply on pragmatic outcomes that are important to the clients (patients).

Techniques for using EBP range from the individual (single clinicians using the above techniques to keep themselves up to date and find information needed to inform specific patient problems); to huge organisations designed to provide systematic summaries of the evidence ("systematic reviews", "meta-analyses", or "guidelines"). These organisations include the Cochrane Collaboration (a vast international network of people dedicated to systematically reviewing the medical literature for clinicians, and setting out their work in a special electronic library, the Cochrane Library www.thecochranelibrary.com, to which Australia has bought a national subscription to make it available to all nationals); various guidelines generating bodies (www.guideline.gov); and the Campbell Collaboration (www.campbellcollaboration.org) which has a focus on non-clinical outcomes.

3 Limitations of evidence-based practice

EBP is not a panacea for helping with decisions. Clearly 'garbage in – garbage out'; that is, if there are no good data to summarise, then it not possible to derive good summaries. Some specific concerns are included in the following lists of problems:

- Inadequate numbers of studies
- Wrong end-points
  - Often the things that we want measured are not measured – and only the things easy to do so are.
- Studies conducted in the wrong population groups
  - There is complicated science attached to 'generalising' from the study groups studied to the setting in which the question was asked.
- Poor study design
  - If the primary studies are poorly designed, then the summaries can be worthless. Different question types (*meaning treatment, diagnostic; prognostic; phenomenological* or *frequency*, for example, require quite different study types (eg RCT, cohort studies, case-control studies, or qualitative studies). Sorting these out requires epidemiological skills.
- Publication bias
  - If only some data are available for analysis (particularly if biased in one direction – such as no effect) then a bias will be introduced to the result.
- Slavish adherence to the results obtained
  - It is easy to criticise EBP as being formulaic, straight-jacketing decisions into a limited set of factors. This would be to over simplify the uses of EBP, which should only be used as an adjunct to the decision-making process. Other factors have to be added in: the weight and preferences of the different options; the cost of alternatives; and other local factors.

4 An example: managing a potential viral pandemic

4.1 Background

Australia is at risk of a viral pandemic. This could be in the form of a hitherto unknown virus such as SARS (Severe Acute Respiratory Syndrome), such as crippled the Asian and Canadian economy in 2003 caused by a coronavirus which affected about 8000 people worldwide, of whom nearly 1:10 died. A new avian influenza pandemic caused by the H5N1 virus strain threatens greater catastrophe.

Naturally, national plans have been developed to address the possibility of H5N1 virus mutating from its form which is highly contagious to birds to one which is to humans. They include three main interventions:

1 **Vaccination of the population**

Unfortunately the highly unstable nature of the outside of the influenza virus renders this hard to prepare in advance. The chance of there being sufficient time to prepare for such a pandemic is tiny.

2 **Stockpiling antiviral drugs**

Unfortunately these are very expensive, and have only slight effectiveness against influenza

a. only a minority of people treated with them gain any benefit; and

b. resistance to the drugs can be rapid.

3 **Physical barriers of hygiene methods**

There are some reports that these may be effective, and, being cheap and relatively easy to implement at short notice, it was judged important to identify the evidence for this measure.

Accordingly a small international group of us decided to systematically review the literature to bring together all the evidence on this last question.[2,3]

4.2 How we did it

First we set out our methods a priori to minimise any subjective distortion (bias) of the results. The principles are essentially those of the '4 As' above. We set some questions, undertook a large electronic search of the literature, appraised the risk of bias among those items of research identified, and showed how these results could be applied to a pandemic.

The search (diagram 1) found thousands of studies, of which only 51 were satisfactory. They contained both randomised and non-randomised trials, and some observational studies as well. We used explicit criteria to establish how to decide how likely the data were to be biased.

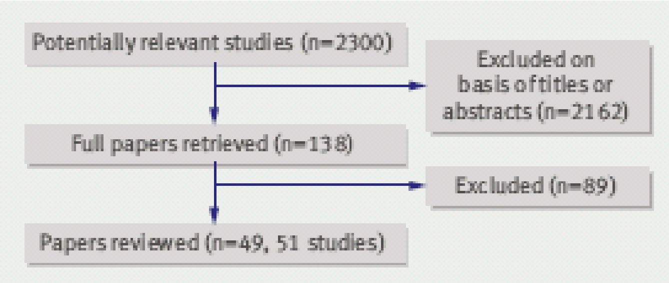

Potentially relevant studies (n=2300)
Excluded on basis of titles or abstracts (n=2162)
Full papers retrieved (n=138)
Excluded (n=89)
Papers reviewed (n=49, 51 studies)

Diagram 1. Searching the studies

4.3 What we found

A variety of different physical methods had been assessed. Hand-washing, wearing gloves, masks and gowns were unexpectedly effective, used separately and even more so in combination. Interested workshop attendees are referred to the references for the specific details. In summary, we found that for every three people using all barrier methods (simple masks, handwashing, gowns and gloves) one case of viral transmission would be prevented.

5 Conclusions

The methods of EBP can be transferred to questions of national security usefully, providing some quantitative estimates of the relative benefits or harms of interventions to confront serious threats to Australian national security. It is astonishing such techniques are not used more frequently, and shared with the data from other countries to provide the best information at the point of decision-making. These techniques are not infallible, but they surely represent an attempt at least to find the best available information to bring to the point of making decisions.

References

1. Sackett DL, Straus SE, Richardson WS, Rosenberg W, Haynes RB. Evidence-based medicine. How to practice and teach EBM. 2nd ed. Edinburgh: Churchill Livingstone, 2000. 250 pages
2. Jefferson T, Foxlee R, Del Mar C, Dooley L, Ferroni E, Hewak B, et al. Interventions for the interruption or reduction of the spread of respiratory viruses. Cochrane Database Syst Rev 2007:CD006207.
3. Jefferson T, Foxlee R, Del Mar C, Dooley L, Ferroni E, Hewak B, et al. Physical interventions to interrupt or reduce the spread of respiratory viruses: systematic review. BMJ 2008;336:77-80.

3

Evidence-based policy in the age of spin: On politics and truth

Robert Watts[1] and Greg Marston[2]

[1]Professor, Discipline Leader Social Sciences, School of Global Studies, Social Science and Planning, RMIT University, [2]Senior Lecturer, School of Social Work and Human Service, University of Queensland

Abstract

The current enthusiasm for what is called ‘evidence-based policy’ may doubtless be explained by advocates for what can variously be called a ‘sociology of knowledge’ or a ‘politics of knowledge’. This kind of interpretative frame would point to ‘evidence-based policy’ as one response by policy communities to the problems of securing legitimacy for public policy interventions in a time characterised by a putative crisis of legitimacy, brought on by advocates of ‘neo liberal’ or ‘public choice theory’. While there is value in pursuing that kind of reflexive critique, there is arguably value in also exploring in a more fundamental way the relationship between politics, policy and theory/knowledge. Such an enquiry would necessarily engage a series of long-standing conventional ideas like the role of truth in politics, the distinction between “facts” and “values”, or the value of the division of labour between experts (and their expert and objective scientific knowledge) and politicians and their management of opinion in the craft of politics. And secondly there is no less compelling evidence that political persuasion works best when it pays attention to people’s values and feelings. Our focus here involves exploring the conventional idea that shaping public opinion or making policy ought properly entail rational persuasion based on appeals to evidence and that rational persuasion based on appeals to evidence provides the gold standard for thinking about politics and policy making.

Keywords: evidence-based policy, policy making, politics, policy, theory, knowledge, values

> The point is only that a fact, an event can never be witnessed by anyone who may want to know about it, whereas rational or mathematical truth presents itself as self-evident to everyone endowed with the same brain power; its compelling nature is universal, while the compelling force of factual truth is limited; it does not reach those who not having been witnesses, have to rely on the testimony of others, whom one may or may not believe. The true opposite of factual, as distinguished from rational truth is not error or illusion but the deliberate lie. Hannah Arendt: 1975: 59

Among the many surprising aspects of contemporary policy-making, and politics more generally, is the current enthusiasm for evidence-based policy. Advocates for evidence-based policy advance the apparently straight-forward proposition found eg., in now-classic statements by Britain's Cabinet Office (1999a; 1999b) that policy makers should be guided by evidence in both the 'discovery' of problems meriting policy responses and/or in the evaluation of the effectiveness of existing policies and programs. Although it hasn't quite swept the field in the way the enthusiasm for 'quality' has done (Oancea & Furlong, 2007:120) this enthusiasm looks as if it needs to be taken seriously now, if only because there is now at least one academic journal (*Evidence and Policy*) devoted to promoting the idea.

This enthusiasm is curious as we propose to show here, because the evidence-based policy movement raises some quite fundamental questions about contemporary public affairs and the politics of policy-making in Australia. That the enthusiasm is curious is suggested by one preliminary question which we (Marston & Watts 2003) have already raised. Does the current enthusiasm for evidence-based policy, and the suggestion that this is either a very modern idea and/or a novelty, imply that policy-making in the past was not evidence-based but rather was based eg., on gossip or innuendo?

Leaving aside –briefly- the question of what might be meant by 'evidence', this implication should not be taken all that seriously. Even the most cursory history of the evolution of policy-making in Anglo-American countries over the past two centuries would point to the considerable and long-standing reliance by modern governments on formal processes of research and systematic gathering of evidence by experts, committees of inquiry and academic researchers. This reliance was on display in 1832 as Britain's Royal Commission on the Poor Laws of 1832 employed political economists like Nassau Senior and Edwin Chadwick to use early versions of social surveys, gathered statistics and drew on the testimony of'expert' witnesses. By the 1840s social statistics of various kinds were being routinely produced and consumed by governments across Europe and in their colonies (Watts 2003). Does this consideration already suggest something about the way an idea like 'evidence-based policy' needs to be put in context? We think so, hence our intention to critically appraise the idea of evidence-based policy, with a view to establishing if evidence-based policy can live up to its promise as an idea whose time has come

(Young et al., 2002).

In particular the question of whether and by what means the advocates of evidence-based policy believe that relying on 'evidence' somehow overcomes certain basic problems in the vexed relationship between knowing ('theory') and doing ('practice') to say nothing of politics and truth point to certain fundamental problems. Our starting point is that whatever merits the natural or social sciences possess as sources of adequate knowledge of the world, we need to accept two things: firstly there is a fraught relationship between knowing and doing: as philosophers like Hannah Arendt (1958; 1974) and Mary Midgley (2001) have understood there so no guarantee that knowing something adequately will lead to good practice or framed in the negative help to avoid wickedness. As we will suggest apropos hard cases like evidence based-medicine, the fact that doctors know that some therapy is scientifically recommended does not mean as Gawande (2007: 25-39) reminds us, that they will actually put it into practice. Secondly and given the suspicion that those appealing to evidence based policy are making some claim that policy-making itself is already, or might become a 'science' (Grayson 2007) we probably need to agree withYoung, et al. (2002: 215) when they observe that this claim may refer somewhat ambiguously either to 'to the way in which policy is made … [or] to the evidential nature of social science itself'. Either way this proposition has been contested quite sharply by Mulgan (2005: 224) when he suggests that in 'a democracy, the people and the politicians have every right to ignore evidence'. To put this bluntly most if not all policy-making exercises are ultimately and necessarily political processes (Rose 1999; Edwards 2000; Bessant et al 2006). This suggests that there is more at stake here than a somewhat narrow and typically academic preoccupation with issues of methodology such as occurs when social scientists adjudicate the merits of various styles or research, research methodologies or evaluate 'data'. Equally this does not mean that we can avoid addressing some hard questions about the relation of politics and truth.

In addressing several questions we think that matter, we begin by exploring the idea of evidence-based policy. Finding a coherent account of evidence-based policy is a difficult task. In much of the policy literature the meaning of 'evidence' and 'evidence-based policy' is treated as if it is either self-explanatory or else is collapsed back into one form or other of a narrow band of 'empiricist' or 'quantitative' research methods. As we suggest here far more is at stake than some methodological squabbles. If we take seriously the ideas of putting evidence-based policy back into its context then we cannot help but observe that any discussion of evidence-based policy needs to engage the fundamental relation of knowledge, truth and politics.

As is now notorious in 2002-3 the governments of the United States, the United Kingdom and Australia mobilized popular support for and then legitimized their subsequent invasion of Iraq by claiming that the regime of Saddam Hussein in Iraq possessed weapons of mass destruction.[1] These regimes claimed that their intelligence

[1] The case for invasion rested on the claim that Iraq had missiles, nuclear capability and lots of

agencies had evidence contained in dossiers pointing to the existence of WMD. How curious that this evidence proved chimerical. This was not surprising given the unfortunate fact that there were no WMD. Equally unsurprising was the unstinting and costly effort to successfully mobilize public (ie., media) opinion in favour of an invasion. As Rix (2008: 61-73) argues this case is considerably amplified when considering the way intelligence agencies have tried to garner evidence in regard to 'terror suspects' like Mohamed Haneef or Izhar Ul-haque in Australia.

This sheds an interesting light on the political and policy use of evidence, and opens up a series of interesting questions about the character and role of evidence in contemporary policy-making processes more generally. Certainly as writers like Rose (1996) have suggested, the relationship of evidence to fantasy evident in state policy exercises may need to be taken more seriously than simple-minded empiricists seem able or willing to consider. Indeed it seems to us that any consideration of the enthusiasm for evidence-based policy in a context in which it seems that modern politics is more concerned with 'spin' than truth points to a number of problems about the interaction between politics and knowledge in which some conception of truth remains as Arendt (2005: 5-8) suggested a vital issue in the practice of politics and the practice of persuasion. At stake as we show are serious questions about truth, political judgment and the strange usages to which evidence can -and cannot- be put.

Let us start with the idea of evidence-based policy itself.

1 The origins and context of evidence-based policy

The term 'evidence-based policy' has evolved from the concept of 'evidence-based practice', both of which were preceded by 'evidence-based medicine'. It is worth briefly examining these developments, as this legacy of ideas even now informs the contemporary enthusiasm for evidence-based policy both overseas and in Australia.

Evidence-based medicine (EBM) refers to the process of systematically finding, appraising, and using research findings as the basis for clinical practice. The philosophical underpinnings of evidence-based medicine are clearly those belonging to a broad-church positivism. This is evident eg., in the way *t*he 'golden standard' of evidence gathering in medicine is the randomised controlled trial, which compares treatments with placebos to determine the most effective intervention (The Cochrane Collaboration 2003). The Cochrane Collaboration, first established in the United Kingdom, has been at the forefront of the push for systematic up-

biological and chemical weaponry. The chief source used by the Bush administration in 2002-3 to justify its claims was a low grade technician, taxi driver and fantasist (Drogin 2007) As late as 2002 investigators with the United Nations Special Commission (UNSCOM) like Scott Ritter were confirming (See Stampton & Rauber 2003). The claims vigorously promoted by the American and British governments were accepted by the Australian government. We also now know that the US government spent billions of dollars after 1998 hiring leading PR companies like Beers to promote an increasingly hostile view of Iraq after 1998.

to-date reviews of all relevant randomized controlled trials of health care (Trinder & Reynolds 2000). The results of these systematic reviews are posted electronically on the Cochrane Library to form a searchable database.

The rigorous 'scientific' process of systematically reviewing the effects of health care treatments underpins evidence-based medicine. Widely adopted in the United Kingdom, and increasingly in the United States, evidence-based medicine is used to identify the most appropriate and effective way to promote health and to treat illnesses. In this sense it has both educative and clinical functions (Solesbury 2001). The logic of evidence-based medicine has spread out of acute medicine into allied health professions and then into related areas like social work and human service practice (McDonald 2002).

Yet the take-up of evidence-based medicine has not met with universal approval. Some commentators suggest that evidence-based medicine constrains other forms of scientific research and/or promotes an overly narrow range of research methodologies (Reynolds 2000: 32). These comments are directly relevant to debates about the value of evidence-based policy, as the disciplinary and methodological roots of the 'evidence-based' discourse in acute medicine has implications for how these ideas are transferred to other areas of professional practice, such as policy-making in the human services.

Researchers and policy-makers in Britain have been driving the evidence-based policy movement, aiming to systematically mobilize and use social science research. The Campbell Collaboration, a sibling organization of the Cochrane Collaboration, focuses on social policy research and aims to conduct systematic reviews 'of the best evidence on the effects of social and educational policies and practices' (The Campbell Collaboration 2003). Beyond making systematic reviews electronically available for policy practitioners, evidence-based policy is also seen by some as a way of bringing social science researchers and their work into closer alignment with government decision-making processes (Parsons 2001).

Not surprisingly, there have been vigorous debates in the UK about the implications of this trend, regarding the appropriate relationship between universities and government decision-makers, intellectual property rights and academic freedom.[2] The Economic and Social Research Council, the Britain's leading independent agency for funding research and training in the economic and social sciences, has been caught up in these debates. Commenting on these issues, Solesbury (2001: 4) observes that 'the Economic and Social Research Council has been subjected to the demands of government science policy that views academic research as a means to economic and social development, much more than a cultural end in itself'. These efforts have been coordinated by a number of Economic and Social

[2] In Britain both Liberal Democratic politicians and academics have publicly raised concerns about the increasing practice of government departments amending research reports before publication and contractual conditions that insist researchers seek departmental permission before speaking publicly to the media about research findings (British Educational Research Foundation, 2001).

Research Council funding initiatives. In 1999, for example, the ESRC provided 1.3 million pounds to the Evidence Network - the UK Centre for Evidence-Based Policy and Practice for a period of three years:

> The primary objectives of the Centre for Evidence-Based Policy and Practice are to foster the exchange of research-based evidence between policy researchers and practitioners, and to accelerate the development of methods of appraising and summarising the results of research relevant to policy and practice. It will also aim to improve the quality of research and practice, and through its dissemination function inform and advise those in policy-making roles (Evidence Network - UK Centre for Evidence Based Policy and Practice, 2002).

These objectives are similar to the aims and methods of the Cochrane Collaboration and the Campbell Collaboration outlined earlier, where the intention is to systematically review available research for practitioners working in a range of policy settings.

The Cabinet Office Centre for Management and Policy Studies in the United Kingdom (1999a; 1999b; 2001) has produced a number of strategic documents aimed at 'modernising the policy-making process'. Evidence-based policy is seen as a core dimension of this process. In the 1999 British Cabinet Office *White Paper on Modernising Government,* evidence-based policy is understood as including:

- Reviewing existing research;
- Commissioning new research;
- Consulting relevant experts; and
- Considering a range of properly costed and appraised options.

From the perspective of those advocating for an evidence-based approach, professional policy-making is best driven by 'evidence' of 'what works', following a series of systematic steps (eg., Parsons 2001). In the United States, the US Coalition for Evidence Based Policy aims to 'promote government policy-making based on rigorous evidence of program effectiveness'. The sorts of 'rigorous evidence' the Coalition promotes consist of 'randomised controls' to ascertain effectiveness based on evidence-based approaches that 'have produced extraordinary advances in human health'. The US Coalition suggests that 'in social and economic programs, by contrast, government programs are often implemented with little regard to evidence, wasting billions of dollars and failing to address critical needs of our society' (US Coalition for Evidence Based Policy 2002). In this approach to 'evidence', the term takes on a new meaning as a resource-rationing tool, which goes beyond its educative and clinical purposes outlined earlier.

Underpinning the Cochrane Collaboration and other evidence-based initiatives is the long standing positivist expectation that it is both possible and desirable to attempt to exclude bias through standardized, rational and neutral procedures (Trinder 2000). From outside that perspective the emergence of evidence-based policy is bets understood as an offshoot of the instrumentalist mode of managerial 'reforms' that have infiltrated public administration practices in many western democracies over the past three decades.Trinder (2000) argues that the managerialist emphasis on 'value for money' and a 'focus on effectiveness and efficiency is a central driving force behind evidence-based practice and policy'. In the case of managerial reforms and evidence-based policy, the technical logic is similarly concerned with procedural competence, rather than substantive output.

In Australia, it is clear that evidence-based policy has begun to reshape the social and public policy field, especially in the lexicon of policy-makers working in both the community and government sectors. However in contrast to the United Kingdom, there is no formal coalition or central coordinating 'think tank' actively promoting this agenda at a Commonwealth Government or State Government level. Nonetheless, within and across government departments there are signs that evidence-based policy is being actively promoted across a number of different fields of social policy. In 1998, the Commonwealth Department of Health and Family Services was talking about the need to translate evidence-based medicine into evidence-based policy, which is defined in terms of assisting the provision of safe, cost-effective and beneficial treatments (Whitworth, 1998).Again in the health field, the National Health and Medical Research Council (2003) offers Practitioner Fellowships on the basis that they contribute to 'evidence-based policy development in Australian health systems'. It is not really surprising that the health field has been the first to take up the evidence-based discourse, given the proximity of this profession to acute medicine.

There are plenty of signs that evidence-based policy is being taken up in other areas of public administration.The Department of Family and Community Services (DFaCS) Annual Report 2000-01 refers to evidence-based policy, by way of 'making administrative data more accessible to the Minister, DFaCS staff and the Australian community' (DFaCS, 2001). In this account, evidence-based policy is defined along the lines of accessible information provision for policy-makers and the general public, echoing the aims ofThe Campbell Collaboration. In the area of income support, Centrelink's 2002-05 Business Plan makes a case for Centrelink's being 'a key player in developing and delivering evidence-based policy solutions for customers, client agencies, community and government' (Centrelink, 2002). A Commonwealth Department of Education, Training & Youth Affairs publication on *The Impact of Educational Research* on school education quotes a senior official, who argues that 'schools will only accept changes that are strongly evidence-based' and that 'research helps to de-politicise educational reform' (DETYA, 2000: 190).

In this context, research evidence is treated as a 'neutral' and 'objective' policy tool that is apparently above political ideology. Increased targeting of social policy programs and the shift towards 'outcomes based funding' in the non-government human services sector also provides fertile ground for evidence-based discourse. Non-government welfare agencies must increasingly quantify what they are doing, what works and why. In the human services, evidence-based policy cannot be separated from a broader political context where eg.,

> … efficiency becomes the primary political value, replacing discussions of justice and interest with discussions of what is possible and practical, with means rather than ends, with methods rather than truth' (Smith & Kulynych 2002: 163).

Australian research institutes, funded by the Commonwealth Government, have also begun adopting the language of evidence-based policy. The Australian Institute of Family Studies was funded in the 2000-2001 Federal Budget to undertake a Longitudinal Study of Australian Children. According to the first paper on the project:

> … the Strategy is based on a holistic approach to problem identification, prevention and early intervention, and a commitment to evidence-based policy and practice' (AIFS 2002).

Winter and Seelig (2001: 6) have promoted the idea of evidence-based policy and research in Australian housing studies as involving the use of 'evidence for policy formation'. Young et al (2002: 216) refer to this conceptualisation of research-policy relations as the *knowledge driven model*, where it is assumed that knowledge leads, or at least *should* lead policy.

Actors in the political field have also been drawing on the concept. In Australian federal politics, for example, a variety of leading ALP politicians have espoused the virtues of evidence. Mark Latham (2001) took poll position in 2001 when he began talking up the value of evidence-based policy as part of his promotion of 'welfare reform':

> The myths of the welfare state are based on old ideological ways of thinking, a struggle between government-first and market-first policies. It is now clear that both approaches are flawed. The world has moved on. Welfare policymakers need to look beyond the old Left and the new Right to those evidence-based policies that can end the human tragedy of poverty.

For Latham evidence-based policy represented a useful tool and theoretical metaphor for going beyond political ideology. Latham treated evidence-based policy as a 'neutral' concept where 'hard facts' would speak for themselves in addressing 'human tragedy' and politicians and policy makers would act in the light of the best available evidence.

This brief account of how evidence-based policy has entered the Australian social policy discourse is far from comprehensive. However, it illustrates different manifestations of evidence-based policy and the inroads that it is making into public management and social policy in Australia and other parts of the western world. A simple part of the reason for current interest in evidence-based policy may be explained by the 'common sense' nature of the term. It is difficult to imagine anyone standing up and arguing that policy should not be based on anything but the best available evidence. The idea has an intuitive logic, which helps to explain how the concept is 'naturalized' in a diverse range of policy settings. As Tilley and Laycock (2000: 13) argue: 'rooting policy in evidence has all the appeal of motherhood and apple pie. The rhetoric is cheap and easy'. The term works as a conventional catch phrase synonymous with 'scientific', scholarly' and 'rationality', constituting a rhetorical framework for thinking about modern policy-making and professional human service practice in highly positive ways.

This is especially apparent in the UK and Australia where 'evidence-based policy' is associated with a 'modernising' agenda as policy-making scholars and practitioners assume the mantle of scholarly, and above all else 'scientific' practice. Where once the science of government was treated as matter for universities to organise (signified for example by the establishment of the LSE in 1909 or Bland's establishment of the School of Government at Sydney University in the 1930s), the modern way involves institutional 'partnerships' between governments and universities in entities like the Australian New Zealand School of Government. In this respect, 'the resurgence of evidence-based policy-making might be seen as a re-affirmation of the 'modernist' project, the enduring legacy of the Enlightenment, involving the improvement of the world through the application of reason' (Sanderson, 2002: 1). In sum, the evidence-based policy movement is premised on the simple proposition that scientific research evidence has an inherent value in the everyday politics of policy-making.

Whether 'empirical research' actually assures a sufficiently secure grasp of the social world to deliver reliable insights into that world able to inform good policies is a far more serious question. That the enthusiasm for evidence is both more curious and more paradoxical than might be immediately apparent is suggested by some quite fundamental considerations.

Firstly there is the otological problem itself which begins with how we understand the nature of reality itself and what it makes possible in terms of evidence. Secondly there is the no-less refractory problem posed by the very large body of research evidence much of it from social psychology and communications researchers which says that our capacity or willingness to be guided by evidence is rather minimal.

2 Two problems: reality and evidence

There are two essential problems with evidence, one to do with the nature of reality, the other with the weak capacity of evidence to inform what we know and do.

One goes to the fundamental interplay between what we can call 'reality' and the various modes of knowing it. While various positivists, empiricists and social science methodologists insist there is no problem here, there is no easy way of getting around a number of difficult problems. Most recently Anne-Marie Mol (2002) and John Law (2004) have reminded us that speaking ontologically as it were, reality is messy.

In spelling this proposition out a bit more (and lest it be thought that we are about to launch a post-modernist version of the 'there-is-no-reality-out-there' kind) we need to make it plain that that there are definite processes, relationships, physical things and kinds of practices and ways of life that are 'out there' waiting to be to be discovered or dealt with. Rather the point to be made as John Law (2004: 6) puts it, is the problem that whatever is out there, is not just going to generate technically complications that get in the way of us knowing 'stuff', but that the world out there *necessarily exceeds our capacity to know it.* This is so because whatever is there is often complex and/or incoherent

Anne-Marie Mol (2002) provides an exemplary case study of why and how this is so in the case of the very serious disease called *atherosclerosis.* Atherosclerosis is the extremely common and all too real medical condition now affecting large numbers of older humans in western societies that we might best understand as a bad case of 'blocked arteries'. It is a disease produced by a combination of factors including bad genes, poor diet, the aging process, too much cholesterol, lack of exercise, diabetes, and hypertension. Atherosclerosis can cause pain, disability, organ failure, strokes, heart attacks, vascular disease, gangrene and death.

Mol (2002) offers an exemplary study of one version of this disease called *lower limb atherosclerosis.* Her point is simple. Firstly this all too-real disease does not produce the same symptoms in each patient. This is partly why the variety of diagnostic techniques (including ultra-sound, manual palpation by the clinician, PET scans, angiograms and autopsies of amputated limbs or the whole and very dead body, all demonstrate varying degrees of utility and accuracy when diagnosing the scale of illness and informing appropriate treatments. As Mol shows in some patients with precisely the same level of arterial blockage, there will be excruciating leg pain (or intermittent claudication) while those other patients with the same degree of blockage report no such pain. The variations in the way the disease manifests and the variation in diagnostic capacity are a striking and simple example of the general point: whatever is meant by an 'out-there reality' it does not exist in a singular or coherent way. 'It' ie., reality is inherently or to put it simply it is ontologically messy.

The problem here is less to do with reality and has rather more to do with the way that lots of people who belong to what can loosely be called the European philosophical tradition have and for a very long time thought to treat reality. They have done so in terms that properly deserve the word 'theoretically' seeking to bend reality to their presumptions about the way 'it' ought to be. This theoretical perspective which has its origins in magical and theological thinking add up to a 'metaphysics of presence'. The consequences have not been helpful.

Law (2004: 24-30) points to some of the key problematic ontological assumptions -including the premises of 'out-thereness', 'independence', 'anteriority', 'definiteness' and 'singularity'. Firstly there is the premise that there is a reality and that 'it' is 'out there' beyond us. Secondly reality is assumed to be independent of our actions and especially of our perceptions. Thirdly reality precedes us. Then and more crucially, reality is deemed to be constituted out of definite relations and forms such that it only exists in 'this' form and not in 'that' form. Perhaps most crucially given these assumptions, the metaphysicians of presence have assumed that reality is the same everywhere or that is common. That is, it is or has a singular and coherent status or character and is the same everywhere because of its out-thereness','independence', 'anteriority' and 'definiteness'.

As Law (2004: 31) notes each of these assumptions need to be treated with plenty of nuance and the frequent use of the phrase 'it all depends' when determining the extent to which these assumptions are credible or not'. Law does not draw the predictable conclusions that too many post-modernists have drawn. For a start Law concludes that we need to value a much large number of 'research methods' when seeking to know 'reality'. This is because it matters that we somehow get the relationship between the world and what we do in it in reasonable alignment. What we know and the adequacy of what we know is linked to the quite pressing need to act in a world and to do so in ways that benefit or help us live well rather than killing or harming us.

If we shift our focus away from the 'ontological' to the actual ways we use evidence and the capacity of evidence to change the ways we know and do things then we confront another equally alarming problem. Another quite fundamental problem is raised by abundant evidence gathered over the past half-century or so by social psychologists and communications researchers, that the authority and value long vested in the idea of evidence-based rational persuasion is strikingly compromised by what we know about 'cognitive dissonance' and 'groupthink'.

It will be recalled that Leon Festinger (1957) used the idea of 'cognitive dissonance' to name the problem of how we deal with evidence that directly contradicts what we already know to be the case. Festinger's ground breaking insight began when he began investigating the members of a doomsday cult persuaded by its leader (who had received telepathic messages from the Guardians who flew around in Unidentified Flying Objects (UFOs) and who had direct communications from God that the world would end on a certain day and time. When the anticipated cataclysm failed to eventuate, the cult and their leader faced the problem of 'cognitive dissonance'. (Here the general idea of 'cognition'/'cognitive' refers to a number of things including evidentiary knowledge, attitude, feelings, belief, self-identity and behavior: any or all of these elements can come into conflict). As Festinger suggested the cult members faced the issue of what to do when something they devoutly believed in, in this case a prophesy fails. He suggested that they had a few options open to them including ignoring the dissonant evidence (ie., the world had not ended) or to add new consonant evidence. On this occasion the cognitive dissonance was resolved when the leader announced that she had received a 'telepathic message' from the Guardians explaining that her cult had done so much good work in preaching the message that God had spared the world).

Since Festinger's original research there has been a lot of research effort put into exploring the very complex ways people select and use evidence-based information to inform their views of the world, to make judgments or to act. Janis' (1984) account of the role played by what he called 'groupthink' in six major American foreign policy catastrophes merely anticipates and indeed may go some way to explain recent security policy failures like the invasion of Iraq. As Janis shows in some detail groups charged with policy-making routinely ignore evidence that does not confirm what they already know or want to do, and use a variety of group processes to silence critics.

Writers like Janis (1953) through to Damasio (2007) have done much to subvert the rationalist premise that humans rely only on rational cognitive processes when they form beliefs, make judgments or act. There is evidence that one of the most important factors that guide people to accept statements as true is the source of the idea: it seems that most us prefer to trust information that comes directly from other people (eg., Johnson 1997; Rintal & Real 2003). Then as Maslow (1963: 111) suggested, we seem to be trapped between 'a need to know and a fear of knowing'. Evidence from the study of public health campaigns designed to get people to change their behaviour (like anti-skin cancer or 'quit smoking' campaigns) suggest that evidence-based marketing campaigns produce complex reactions and are as likely to lead to avoidance of the evidence as to any desired change in behaviour (O'Keefe 1990). That is, the evidence suggest that more of us are more likely to seek out evidence that helps reduce uncertainty or to accept untrue statements that support what we already believe rather than accept or seek out evidence that is accurate or true but that controverts something we know already or that may induce anxiety or stress (Kulthau 1993). Finally there is abundant research evidence which suggests that people screen out evidence or arguments with which they disagree and/or screen in evidence and arguments with which they agree or else use their preferences for one political candidate to accept as true evidence or political marketing material which support a candidate (Iyengar et al 2008).

Much about this body of research resists easy compression or generalisation but it does seem to suggest *inter alia* that 'evidence' largely works in one way ie., it works to reinforce views, theories, self perceptions and beliefs already held, while any strongly dissonant evidence is either rejected or else simply further entrenches views/beliefs facts already believed to be true.

The crucial insight from what is now a very large body of evidence is that the relationship of evidence, emotions and our being in the world is less likely to promote a regard for evidence based-knowledge and activity. It is far more likely to give us cause to avoid information because it distresses us, or because it increases our anxiety, or else is rejected as simply unacceptable because it contradicts what we already know, believe or prefer. Alternatively we simply select the evidence that supports our existing views and press on doing what we want to do.

The actual regard for evidence and its capacity to function as it is supposed to do, that is as a source of rational persuasion is put into a stark light when we recall recent policy research that has informed Australian welfare policy development. This case subverts any conventional thinking about the value of evidence. Indeed this case suggests that evidence that contradicts what is already 'known' and widely believed to be the case is simply not going to be believed or relied on. This seems to have some general features and one, more specific feature.

On the one hand it seems that the Australian social policy community has not been all that able or willing to puzzle sufficiently well about the strange capacity to keep on (re)'discovering' 'poverty'.

The notion of 'rediscovery' certainly overstates both the novelty and the status of these recurrent discoveries. In Australia for example there is a record of persistent research effort undertaken since the mid-1960s into poverty (Encel 1988; 1990; Sitsky 1989). This (re)discovery' raises some basic questions about the social and political significance of income inequality research in contemporary Australian social policy. That there is a point to 'problematising' seemingly 'obvious' processes of discovery such as this, was first raised in Australia by Geoff Sharp. At the height of an earlier 'rediscovery' of poverty in Australia, Sharp (1974) suggested:

> ... it has sometimes been noted that such rediscoveries [of poverty] recur periodically. The clear implication is that the object of discovery has no neutrally independent existence, but has a good deal to do with ethical and social imperatives that find expression through the eye of the observer ...At least initially the emphasis [here] is on why it is being observed and how it comes about that what was previously hidden can be discovered or rediscovered now.

Sharp then posed the question we need to revisit:

> .... [W]hy should we assume that 'the truth' of the existence of poverty is any less ambiguous than the earlier assumption that it 'was no longer with us'? (Sharp 1974: 194)

In effect Sharp is insisting that if it is legitimate to enquire into the distribution of income and the processes that produce poverty, along with the methods for doing this, it is equally legitimate to enquire into the social processes involved in this research and 'discovery' process and their consequent impact on policy development. Here there are many complex issues arising out of the relationship between reality, our knowledge of it and practical interventions like those which take place as policy-makers intervene.

The second and related proposition that goes to the question of the evidence basis of modern welfare policy is suggested when we consider again how what Furedi (2005) calls 'the fear of politics' has successfully invoked the idea that ordinary decent taxpaying Australians have a lot to fear from something called the 'underclass' a large group of 'welfare dependent' spongers. Bessant (1995) recalls the role played by some social scientists, including self-declared progressives in promoting the idea that we should fear welfare beneficiaries,This politics of fear has helped to drive an evolving regime of income support based on stigmatizing categories hyper-surveillance and disciplinary procedures. In that context the most recent phase in the evolution of Australia's experiment in the 'welfare-to-work' legislation that took effect back on 1 July 2006, gives practical expression to the idea we need to fear single mothers, the long-term unemployed or people with disabilities.

There is of course an old provenance to the idea that there are plenty of people out there who are going to take advantage of'us'.This fear has propelled governments to sweep up single parents, older age unemployed and people with serious disabilities and chronic illnesses, and take them off their current typically more generous benefits (eg., Single Parent Supporting Benefits or Disability Support Pensions) and locate them in the far meaner regime of surveillance and activity testing associated with Newstart Allowance.

Of course this is not a new policy. It is a policy that has its antecedents in policy processes that began over 20 years ago (Bessant, Watts et al 2006). The waves of Howard government 'welfare reforms' were but one of a series of social security 'reforms' going back to the so-called 'active society' model first spelled out by the OECD Social policy secretariat ca., 1984-6. The Howard government 'reforms' simply built on the work of its ALP predecessors beginning with the trialing of a 'work-for-the-dole' scheme in 1997 followed by another major review process producing the McClure report of 2001 which spelled out the 'new' doctrine of 'mutual obligation'.

Central to that doctrine as it had been central to the welfare reform process stretching back to the mid-1980s was the core belief that what had once been a problem of 'unemployment' had become a 'problem of 'the unemployed'. This policy process has relied on assiduously promoting the US style critique of the core category of 'welfare' which permitted the representation of the problem as the 'problem' of 'welfare dependency'. "Welfare dependency' became the modern way of talking about the persistence of a class historically referred to as 'paupers' and later as the 'undeserving poor'. 'Welfare dependency' creates unsustainable fiscal burdens on hard working taxpayers. According to this narrative 'welfare dependency' led to life in an 'underclass' of loafers, criminals, addicts, and the mentally ill. It is the very expression of anti-social disorder and immorality. This move relied on social science-based representations of unemployed and low income people as different from 'ordinary Australians' and possibly even a threat to our economy and certainly to the ethical order that the regime of wage work had for so long served to embody and to secure.

Our point is that there is plenty of evidence to show that this portrait is simply mistaken as Peel(2003) argues. The most significant evidence is the empirical survey undertaken by the then-Department of Family and Community Services (DFACS). This was research work done to support the McClure Committee established in 1999 to make recommendations on 'welfare reform' to the Howard government. This research undertaken in 1999-2000 surveyed a large number of income beneficiaries. It was buried in a technical appendix to the Interim Report of the McClure Committee released early in 2000 and was available only on-line.

This substantial body of data on the characteristics of Australian income support beneficiaries showed that in terms of labour market participation or civic engagement 'they' were no different from 'us' ordinary Australians. This evidence, buried in a Technical Appendix to the McClure Interim Report was not allowed to stymie the official view that the essential problem was the problem vested in the character and life style of welfare beneficiaries which sustained the problem of 'welfare dependence'. On this occasion the evidence had to be repressed and prevented form affecting the outcome of the policy process.

This discussion has so far pointed to a general problem. We seem to be immune to rational evidence-based arguments designed to change our minds or our behaviour. There is also the effects of the peculiar way we now do politics.

3 Evidence-based policy in an age of spin

The coincidence of the commitment of governments, including Britain's Blair government and the Howard government, to both evidence-based policy *and* to the politics of spin is surely of great interest. The extent to which this conjunction involves a contradiction, or simply points to combinations of hypocrisy or stupidity is a moot question given the primacy now accorded to ceaselessly gathering data about the state of public opinion provided by relentless polling most of it generated by and then reported in the media.

Campbell's (2007) insider's account of how the 'politics of spin' worked in Whitehall points to the serious consequences for politics itself. Ballard (2007: 100) eg., is not alone when he observes how modern politics has been reconstituted for the age of cable TV news. The result is a politics reliant on:

> … fleeting impressions, an illusion of meaning floating over a sea of undefined emotions … a virtual politics unconnected to any reality, one which defines reality as itself [and one in which] the public willingly colludes in its own deception.

Bourdieu (2008: 189) with his characteristic acerbic ability to get to the point characterises modern politics as a process in which politicians:

> … enclose themselves ever more in their hermetic pursuit, often with no other communication wit the outside world except polls that produce responses by the very questions they impose, and a number of them, moved solely by a concern to simply exist (like pretenders) or survive (like dethroned champions), mutually determine one another in actions that, far from being based on ethical conviction or devotion to a political cause, are no more than reactions to the reactions of others. The peak of perversion is reached when, with television performance becoming the measure of all things, communication advises guided by opinion pollsters train politicians to mime sincerity and play at conviction.

The consequences for political life of this preoccupation with 'evidence' and the role played by government agencies in developing a 'politics of fear' (Furedi 2006) is suggested when we recall the widespread sense that we now face unique new threats to our security.[3] The practical consequences of this as Agamben (1999; 2004) has argued, include moves by western states to suspend the rule of law and create states of exceptionality (involving the reintroduction of state-sanctioned torture (Danner 2007). The means by which fear is manufactured has been superbly documented by Marr and Wilkinson (2006) in their forensic account of the systematic exercise orchestrated by the Howard government in September 2001 to mislead the Australian people about the rationale for their handling of the request by the *MV. Tampa* to transfer a number of asylum seekers they had rescued from a sinking boat.

Marr and Wilkinson remind us of what is at stake. In this case the Howard government's use of ostensibly 'objective' images of babies apparently being thrown overboard, help to frame a sharp question or two about the nature of evidence and the capacity of seemingly objective things like photographic images to deceive or mislead. Here Daston's and Gallison's (2008) account of the history of the idea of 'objectivity' and the variety of practices said to generate or guarantee it, points if nothing else to the problematic authority vested in photographic techniques as a guarantee of what they call 'mechanical objectivity').

This line of enquiry insists that we think more and better about the relationship between politics and truth.

If the contemporary 'politics of fear' works by conjuring up 'evidence' of states of affairs that are not quite what they seem, then there are no less interesting questions about how it is possible that robust evidence that something is there is ignored. Our own interest in Australian social policy and the way that the doctrine of 'mutual obligation' has been validated provides some rich material for reflecting on this problem. The salience of this is suggested for example how it is possible that relevant evidence on the levels of social participation of welfare beneficiaries is systematically repressed.

In effect on this occasion this use of evidence is properly the other bookend to the case of the evidence alleging Iraq's possession of WMD. In the case of WMD there was no possibility of there being evidence for the existence of WMD in Iraq.

[3] If public opinion polls are to be believed for example, many Australians believe that the world is not a safe place anymore and we need to defend ourselves from terrorists intent on destroying 'the Australian way of life' or attacking 'the West'. Many Australians appear to accept that they are engaged in a 'war against terror' waged by 'radical' or 'fundamentalist' Muslims that began with the 9/11 attacks on New York and Washington in 2001. Australia joined with the USA and Britain in a 'Coalition of the Willing' first in an invasion of Afghanistan in 2002 and then of Iraq in March 2004 apparently to prevent Iraq using its arsenal of 'weapons of mass destruction' against the West. In August 2005 an A.C. Nielsen poll showed that 70 % of Australians expected a terrorist attack in Australia in the 'next few years'. In January 2006 one news poll had 87 percent of those surveyed fearful about terrorism. FOXTEL TV news polls in August 2005 and again at the end of 1007 suggested that more than between 80 percent and 90 percent of Australians were prepared to relinquish most of our civil liberties in order to have stronger security laws.

The proposition that there were WMD required as Campbell (2007) allowed that this case be 'sexed' up. In the case of welfare reform the opposite problem confronting the relevant government was that the evidence generated for the McClure Committee directly contradicted what the government and indeed the McClure committee already knew. It had to be repressed

In effect this juxtaposition of spin and evidence raises in alarming fashion certain problems of 'political practice' and what we might properly call here the 'politics of truth'. One good way of establishing what the problem is begins by establishing what the evidence on evidence tells us.

That on the one hand government agencies found evidence for WMD in Iraq (when there were none) and that on the other hand government agencies repressed evidence that Australian welfare beneficiaries were no different from the broader Australian community, reminds us that policy-making communities are no less immune than the rest of us to believing what we already know to be the case and looking for the evidence to sustain these beliefs or else work to repress evidence that contradicts what we already know to be the case. In each case Martin Heidegger has something to add to this discussion and to say something about how we might both think better and do better.

4 Thinking, judging and acting politically: Heidegger

Though it may seem a bit of a stretch to link this discussion of evidence–based policy with the often esoteric and 'difficult' philosophy produced by Heidegger (1962), there are several fundamental points of contact. On the one hand Heidgegger's often forbiddingly abstract account of our being in the world, and the work of later generations of theorists of practice opens up large questions about the complex ways we live in think, judge and act in the world. If Heidegger is rightly acknowledged as perhaps the single most influential philosopher of the twentieth century as Guignon (2006: 1-2), for example suggests, then we need to be able to say why this is the case. Recalling that Heidegger's influence is evident in the work of such varied figures for example as Sartre, Gadamer, Arendt, Geertz, Rorty, Taylor, T.S. Kuhn, Foucault, Manent, Latour and Bourdieu points to certain key propositions with which they started and which Heidegger provided.

Heidegger is important because of his commitment to thinking against the preoccupation with methodology and foundationalist models of scientism which have provided one dominant motif in modern philosophy and the social sciences. The second is his account of how we come to form our understanding of the world in the context of our being (*Sein*) in the world (*Dasein*) and in the context of our habits and forms of practice into which we are largely unconsciously habituated.

At the risk of over-simplifying matters -but in the interests of a needful compression what has been called the 'hermeneutic turn' begins with Heidegger's rejection of what Frede (2006: 42) calls 'substance ontology'. That is Heidegger calls out a long-standing premise which links the earliest of philosophers like

Plato through to classical physicists, namely the idea that there is an underlying and enduring 'presence': this is as Guignon (2006; 4) points out, what links Plato's Forms, Aristotle's 'primary substances', Descartes' *res extensa,* Kant's *noumena* or Newton's grounding his physics in objective time, space and gravity into a persistent 'metaphysics of presence'. However it also generates a series of puzzling binaries which philosophers have endlessly and fruitlessly tried to resolve through debate: at stake are the merits of mind/matter, idealism/realism, facts/values or objectivism/subjectivism. Heidegger undercut this tradition by focusing on 'being' (Sein) and in particular on the way humans actually live out their *Dasein* or 'being there' ie., the ways we live our lives in specific historical life-worlds a state of being. Our being there comes before our will to theorize and abstract starts to take us away from that state of being, Heidegger's 'new' ontology focused instead on the very conditions of intelligibility or understanding whereby we come to be in the world and do so by engaging in constant, intelligible pre-theoretical practice beginning with our use of language.

Heidegger's project began with his recalling the ways we live in the midst of our practical day-to-day activities before we have learned to split mind and matter. This involves him in rejecting any idea of achieving or finding a pure or neutral point of view form which we can gaze in on ourselves by adopting what Manent has called the spectator view advocated by successive realists, naturalist and positivists. Rather Heidegger insists that we start with our own 'life-world' and the ways this 'embeddedness' in a world of practice enables us to engage intelligibly in the world. Hence Heidegger's famous interest in mundane practices like turning a doorknob or hammering away in a workshop. This it should be noted in no way sanctions a retreat into any kind of complacent common sense: rather Heidegger insists on the need to interrogate the fundamentally tragic unfolding of our lives between the moments of our birth and death: Our being in time adds an uncomfortable indeterminacy since as Heidegger puts it 'My being –who I am – is nothing other than what unfolds in the course of my life'. Our agency is constantly at stake as we seek to understand a life which is lived forwards but only on the basis of understanding backwards even as we live forwards: this is a life lived on the edge of an 'abyss' (or *Abgrund* ie., an absence of ground). There is no way out of this 'hermeneutic circle' and certainly methodological escape hatch. Philosophers may have dreamed of finding a secure vantage point from which to get at reality 'as it really is' but there is no escaping the 'hermeneutic circle' The search for constants, regularities and predictive certainties is a chimera undone by our radical 'situatedness' in time - which for all of us eventually runs out. As Guignon (2006: 11) puts it:

> … though our general sense of things depend on what we encounter in the world, we can first discover something as significant … only because we have soaked up a 'preontological understanding' of how things in general can count, through being initiated into the practices and language of our culture.

In short the 'hermeneutic turn' involves the rejection of abstracted (natural) scientific rationality as the only or best source of cognitive and evaluative authority. It also sanctions a resolute rejection of an undue preoccupation with epistemological questions and certain abstracted theoretical criteria for determining what is 'rational'. It begins with the idea that what we know and do is grounded in and made possible by our entry into an historical community of practice -beginning with our immersion in a pre-given linguistic and conceptual worldview or field of discourse. As Gadamer (1994) who deepened Heidegger's account in useful ways argued insisted we confront a diversity of ways of knowing, grounded in what he called our historical nature including certain fundamental intellectual or disciplinary prejudices or what Gerald Holton (1984) called *themata* which are at work in all the variety of modes of human cognition and practice from art and poetry to physics and mathematics.An important entailment of this framework is the proposition that whatever gets to be selected or counted as evidence depends on these *themata*.

5 Conclusion

Hopefully enough has been said here about the ontology of being (and mindful of the notoriously abstracted and 'difficult' language Heidegger invented to talk about this), we can see what is at stake here for any account of politics and policy-making.The evidence on evidence suggests that evidence works in two ways: either to persuade people of what they already know/believe to be the case or else to persuade them that they evidence presented to them which contradicts what they already /know believe must be rejected and or confirms them they are already possessed of a true belief or accurate knowledge. Heidegger's 'hermeneutic turn' points to the power of our life-world and the habits and practices that dispose us to think, act and feel in certain ways.

Yet we are still faced with basic questions and problems that link what we know and think to what we do. How do we do this? One of the essential points of linkage here is the obvious fit between a conception of reality as inherently messy (Law 2004) outlined above, a conception of the value however limited it may be of applied research and the need to live and make do in an inherently messy world filled with a plurality of ethical ideas, and practices and ways of knowing. At stake here is the practical and ethical problem of how to link theory/knowledge and politics/policy. One way forward has been suggested by Arendt (2005) and Flyvbjerg (2004) who have argued for good judgment -or *phronesis*.

The recovery of an interest in *phronesis* a concept developed by Aristotle, has been underway since the recovery of virtue ethics in the 1970s (eg., Anscombe 1968; MacIntyre 1986) and as Arendt (2005) absorbed it into her theory of the political and as it has been promoted subsequently by Nussbaum (1986) and Flyvbjerg (2004) as a framework for contemporary policy and professional practice.

Aristotle (1975) understood *phronesis* as a basic human virtue (ie., as something we can aim at being excellent at). The idea of good judgment (*phronesis*) Aristotle understood as a particular kind of practical intellectual virtue: that is, knowing how to act in specific situations. As such it is something we can be socialised or trained in, just as we can practice it and get better at it. Good judgment relies on practice, for as Damasio (2006, xix) observes, it:

> …depends on how well we have reasoned in the past; on how well we have classified the events of our past experiences in relation to the emotions that preceded and followed them; and also on how well we have reflected on the successes and failure of our past intuitions.'

Good judgment involves an orientation or disposition to act truthfully and with reason in the practice of deliberation and is oriented to practical action in which some conception of the good is at stake. It is best understood by reference to Aristotle's (1975: 1139a; pp. 27-8; 1178b pp. 20-22) threefold distinction between ways of being or acting in the world. Firstly there is *theoresis* (involving profound concentrated contemplation a little akin to meditation); then there is *poiesis* (involving production or world making) and finally there is *praxis* or social action Each of these ways of being and acting in the world is linked to a kind of knowledge there is *episteme theoretike* (or theoretical knowledge achieved by various styles of valid reasoning); there is *techne* (or technical skill) involving a trained capacity for action and finally there is *phronesis* or practical wisdom. Each of these are different yet complementary capacities and ways of knowing and being in the world.

Translated into present-day language good judgment refers to a practical wisdom that is more than simply knowing about principles of action. Good judgment refers to a practitioner having the wisdom that come though experience to make good judgment and to know how and when to act in ways that will promote the basic goods. Good judgment refers to an ability on the part of the practitioner to know when and in what ways to act courageously, honestly, or generously. It refers to the ability to know how and why what might be an act of courage in one context is high risk or reckless in another. This means being both context sensitive and able to judge what the right measure of an action is. (Arostotle spoke often about a golden mean" think of a virtue like 'courage'. Too little is the vice of 'cowardice' too much is the vice of foolhardiness.

To speak about the pursuit of goods reinstates a proper regard for knowledge. To say how we may think about good judgement entails accepting first that knowledge is a fundamental and universal human good. John Finnis (1980) provides one of the most compelling modern accounts of the nature of knowledge as a good using a kind of analytic dialectic which moves backwards and forwards between assessments of human good and its practical requirements *and* explanatory descriptions using historical, experimental, and sociological materials and methods. This good he (1980: 60) says, is grounded in a very common human activity, namely the 'activity of trying to find out, to understand and to judge matters correctly'. As he (1980: 61) puts it:

> Commonly one's interest in knowledge, in getting to the truth of the

> matter, is not bounded by the particular questions that first aroused one's desire to find out … In explaining, to oneself and others, what one is up to, one finds oneself able and ready to refer to *finding out, knowledge, truth* as sufficient explanations of the point of one's activity, project or commitment. One finds oneself reflecting that ignorance and muddle are to be avoided … 'it's good to find out…' now seems to be applicable not merely in relation to oneself … but at large … and for anyone.

Finnis (1980: 65) proposes that knowledge is a human good and there are no sufficient reasons for doubting that this is the case. He allows that the truth of this claim 'cannot be demonstrated, but then it needs no demonstration'. It is simply self-evident. Or rather as Finnis (1980: 74-5) proceeds to suggest, any scepticism about the basic value of knowledge is self-defeating or self-nullifying.

The second basic idea is that *phronesis* is a deeply practical capacity. Those who work in this tradition stress the need to be good at practical deliberation addressing the question 'what ought I do in this case?' This question necessarily arises in the contexts of our daily lives with other people. An orientation to phronesis suggests that addressing and answering ethical questions has less to do with philosophical analysis and much more to do with being a good person who can in each circumstance try to exercise good judgment.

It is against this backdrop that Arendt's relentless attempt to specify what it is that marks out politics as our highest accomplishment and the challenge it daily poses to think well and to do well takes its salience. The need to do so arises in Arendt's mind (2005: 93-5) from the fact of difference between us ie., the fact of human plurality This means for her that there is no human essence and no essence of politics: politics is what arises between men. On the one hand she notes the inevitability of prejudices which constitute our life world

> The prejudices that we share, that we take to be self evident, that we toss out in conversation are… political in the broadest sense of the word, that is, something that constitutes an integral part of those human affairs that are the context in which we go about our daily lives. That prejudices play such a large role in daily life and therefore in politics is not something that we should bemoan as such, or for that matter attempt to change … men cannot live without prejudices … (Arendt 2005: 99)

(Arendt suggest that to attempt to overcome all our prejudices would require 'a superhuman alertness') Equally the task of politics involves distinguishing between genuine prejudices and acknowledging the requirements of good judgment: our substitution of prejudice for judgment becomes dangerous only if it spreads into the political realm where we cannot function at all without judgement(2005:101). The practice of judgment relies in her luminous phrase on developing both our capacity and will 'to think what we do'.

The implication of this discussion for a consideration of the current enthusiasm for evidence-based policy is simple. Thinking well trumps evidence: the practice of good judgment comes prior to the mindless conviction that anything can be measured. While evidence-based policy may be a boon to any number of university-based researchers we need to exercise a duty of care to think about the effect of this not least of all on universities and on our policy-making communities.

References

Agamben, G., 2005, *States of Exception* (Trans. K. Attell), University of Chicago Press, Chicago.

Agamben, G., *Homo Sacer: Sovereign Power and Bare Life*, University of Chicago Press, Chicago.

Arendt, H., 1958, *The Human Condition*, HBJ, New York.

Arendt, H., 1975, *The Life of the Mind*, HBJ, New York.

Arendt, H., 2005, *The Promise of Politics*, (ed J., Kohn), Schocken, New York

Aristotle, 1975, *Ethica Nichomachea,* (Vol IX), *The Works of Aristotle,* Oxford University Press, Oxford,

Australian Institute of Family Studies, 2002, *Introducing the Longitudinal Study of Australian Children*, [Online], Available: http://www.aifs.gov.au/lsac/pubs.html [2002, May 16].

Ballard, J.G. 2007, *Kingdom Come*, Fourth Estate, London.

Bessant, J., 1995, 'The Discovery of a Juvenile 'Underclass', *ANZJS,* vol36, (2) 55-72

Bessant, J., Watts, R., Dalton, T., & Smyth, P., 2006, *Talking Policy: How Social Policy is Made.* Allen & Unwin, Sydney.

Bourdieu, P., 2008, *Political Interventions: Social science and Political Action*, Verso London

Cabinet Office, 1999a, *Modernising Government*, Cm 4310, The Stationery Office, London,

Cabinet Office, 1999b, *Professional Policy Making for the Twenty first century*, Strategic policy making Team, Cabinet Office, London,

Campbell, A., 2007, *The Campbell Diaries*, Random House, London.

Centrelink 2002, Centrelink's 2002-2005 Business Plan, [Online], Available: http: www.centrelink.gov.au/internet/internet.nsf/filestores/pr108_0207/$file/pr1008_0207en.pdf [2002, Jan. 17]

Certeau, M. de, 1988, *The Practice of Everyday Life,* UCLA Press, Berkeley.

Coalition for Evidence Based Policy 2000, *Mission and Agenda,* [Online], Available: **www.exelgov.org/performance/evidence/execsumm.htm**

Cook, F. 2001, *Evidence-based policy making in a democracy: exploring the role of policy research in conjunction with politics and public opinion*, paper prepared for delivery at the 2001 Annual meeting of the American Political Science Association, San Francisco, August 30-September, 2, 2001.

Damasion, A., 2007, *Descartes' Error,* (2nd ed) Grosset-Putnam, New York.

Daston, L., & Gallison, P., 2008, *Objectivity,* Zone Books, Brooklyn.

Department of Family and Community Services (DFaCS) Annual Report 2001

Drogin, B., 2007, *Curveball: Spies, Lies and the Con Man who Caused a War,* Harper, New York.

Edwards, M., 2001, *Social policy, Public Policy: From Problem to Practice*, Allen & Unwin, Sydney.

Evidence Network - UK Centre for Evidence Based Policy and Practice, 2002

Evidence Network 2002, *The History of Evidence Network*, [Online] Available: http://www.evidencenetwork.org/history.asp [Dec. 6, 2002].

Festinger, L., 1957, *A Theory of Cognitive dissonance,* Stanford University Press, Stanford.

Finnis, J. 1980, *Natural Law and Natural Rights*, Oxford University Press, Clarendon.

Flyvbjerg B., 2004, *Making Social Science Matter,* Cambridge University Press, Cambridge.

Frede , D., 2006, 'The Question of being: Heidegger's project, in . Guignon. C. 2006 (ed.), *The Cambridge Companion to Heidegger* (2nd ed) Cambridge University Press, Cambridge

Furedi, F., 2005, *Politics of Fear: Beyond Left and Right*, Continuum, London.

Gawande, A., 2007, *Better: A Surgeon's notes on Performance*, Picador, New York

Grayling, A.C. 2003, *What is Good? The Search for the best Way to Live,* Weidenfeld & Nicholson, London.

Graysion, L. 2007, *Policy makers use evidence Only when it Suits them: Discuss*, Center for Evidence Based Policy and Practice, London.

Greenberg, K., & Lewis, A., 2005, (eds), *The Torture Papers: The Road to Abu Ghraib,* Cambridge University Press, Cambridge.

Guignon. C. 2006 (ed.), *The Cambridge Companion to Heidegger* (2nd ed) Cambridge University Press, Cambridge

Haack, S., 1998*, Manifesto of a Passionate Moderate: Unfashionable Essays*, University of Chicago Press, Chicago.

Haack, S., 2007, *Defending Science –Within Reason*, Prometheus Books, Amherst.

Hansen, P., 1993, *Hannah Arendt: Politics, History and Citizenship*, Stanford University Press, Stanford.

Heidegger, M., 1962, *Being and Time* (Trans J. Macquarrie & E. Robinson),SCM Press, San Francisco,

Iyengar, S., Hahn,K., Krosnick, J., & Walker, J., 2008, 'Selective Exposure to campaign Communication: The role of anticipated Agreement and Issue Public membership', *The Journal of Politics,* vol 70, (1) pp186-200

Janis, I., 1953, 'Effects of Fear Arousing Communications', *Journal of Abnormal Psychology*, vol 48, pp 78-92

Johnson, J., 1997, *Cancer related Information Seeking*, Hampton Press, Cresskill.

Kulthau, C., 1993, 'A Principle of Uncertainty for Information seeking', *Journal of Documentation,* vol 49, (2), pp 339-55.

Latham, M. 2001, 'Myths of the Welfare State', *Policy,* Vol 17, no 3, pp. 40-43.

Law, J., 2004, *After Method: Mess in Social Science Research,* Routledge Abingdon.

MacIntyre, A., 1981, *After Virtue,* University of Notre Dame Press, Notre Dame.

MacIntyre, A., 1985, *After Virtue: A Study in Moral Theory*, Duckworth, London.

Marr, D., & Wilkinson, M., 2006 *Dark Victory,* (2nd ed.) Allen & Unwin, Sydney

Marston G., & Watts, R., 2003, 'Evidence-based policy: An essay in disruption', *Just Policy,* No 29, July 2003 : 32-48.

Maslow, A., 1963, 'The Need to Know and the Fear of Knowing', *Journal of General Psychology* vol 68 : pp111-25

Mol, Anne-Marie, 2003, *The Body Multiple: Ontology in Medical Practice,* Duke University Press, Durham.

Mulgan, G., 2005 'Government , Knowledge and the Business of Policy Making: the Potential and Limits of Evidence-Based Policy', *Evidence and Policy,* vol.1, (2) 215-226

National Health and Medical Research Council (2003) *Practitioner Fellowships,* [Online], Available: www.health.gov.au/nhmrc/research/train/practfly.htm [2003, Jan. 16]

Nussbaum, M., 1986, *The Fragility of Goodness,* Cambridge University Press, Cambridge.

Nutley, S. Davies, h. & Walter, I. 2002, *Evidence Based Policy and Practice: Cross Sector Lessons from the UK*, Keynote paper for the Social Policy Research and Evaluation Conference, Wellington, New Zealand, 2-3 July.

O'Connor, A., 2000, *Poverty Knowledge*, Princeton university Press, Princeton.

O'Keefe, D., 1990, *Persuasion Theory and Research,* Sage Newbury Park

Oancea A., & Furlong, J., 2007, 'Expressions of Excellence and the Assessment of Applied and Practice based Research', *Research Papers in Education,* vol.22 (2) pp. 119-37

Orwell, G., 1946, 'Politics and the English language', in *Shooting the Elephant and Other essays,* Secker & Warburg, London

Parsons, W. 2001, Modernising Policy-making for the Twenty First Century: The Professional Model, in *Public Policy and Administration*, vol. 16, no 3, pp. 93-110.

Peel, M., 2003, *The Lowest Rung,* Cambridge University Press, Cambridge.

Perri, S. (2002) 'Can Policy Making be Evidence Based?' *MCC Building knowledge for integrated care*, vol 10, no 1, pp. 3-9.

Rampton, S., & Stauber, J., 2003, *Weapons of Mass Deception,* Hodder, London.

Reynolds, S. 2000, 'The Anatomy of Evidence-Based Practice: Principles and Methods', in *Evidence-Based Practice: A Critical Appraisal*, (eds) L. Trinder & S. Reynolds, Blackwell Science, Oxford.

Rintal, R., & Real, K., 2003, 'Perceived Risk and Efficacy Beliefs as Motivators of Change: Use of the Risk Perception Attitude (RPA) Framework to Understand Health Behaviour', *Human Communications Research,* Vol 29 (3) pp. 370-99.

Rix, M., 2008, With Reckless Abandon: Haneef and Ul-haque in Australia's 'War on Terror', in Michael K, & Michael, M., (eds), *Australia and the New technologies: Evidence based Policy in Public Administration,* University of Wollongong, Wollongong.

Rose, J., 1996, *States of Fantasy*, Oxford University Press, Oxford.

Rose, N. 1999, *Powers of Freedom: Reframing Political Thought,* Cambridge University Press: Cambridge.

Rose, N., 1996, 'The death of the Social: Refiguring the territory of Government, *Economy and Society,* vol.25. (3)

Rosenstock, L. and Lee, J. 2002, 'Attacks on science: The risks to evidence-based policy', *American Journal of Public Health*, vol 92, Issue 1, pp. 14-18.

Sanderson, I. 2002, *Making Sense of 'What Works': Evidence-Based Policy Making as Instrumental Rationality?* Paper presented at the Political Studies Association Annual Conference Aberdeen, 5th- 7th 2002.

Shapin, S., 1996, *A Social History of Truth*, University of Chicago Press, Chicago.

Sharp, G., 1974, 'Interpretations of Poverty', *ANZJS*, vol.10, no.3 pp. 194-199.

Solesbury, W. 2001, Evidence Based Policy Whence it Came and Where it's Going, *ESRC UK Centre for Evidence Based Policy and Practice: Working Paper 1*, ESRCF UK Centre for Evidence Based Policy and Practice, London.

The Campbell Collaboration 2003, *About the Campbell Collaboration*, [Online], Available: http://www.campbellcollaboration.org/FraAbout.html [2003, Jan. 14]

The Cochrane Collaboration 2003, *Brochure*, [Online}, Available: http://www.cochrane.org/cochrane/cc-broch.htm [2003, Jan. 13]

Tilley, N. & Laycock, G. 2000, *Joining up Research, Policy and Practice about Crime*, Policy Studies, vol 21, no 3, pp. 213-227.

Trinder, L. 2000, 'Introduction: the context of evidence-based practice', in *Evidence-Based Practice: A Critical Appraisal*, (eds) L. Trinder & S. Reynolds, Blackwell Science, Oxford.

Trinder, L. and Reynolds, S. (eds) 2000, *Evidence-Based Practice: A Critical Appraisal*, Blackwell Science, Oxford.

United States Coalition for Evidence Based Policy 2002, *Program Description*, [Online], Available: http://www.excelgov.org/displayContent.asp?Keyword=prppcProgDesc [Feb, 6, 2002]

Vlastos, G., 1991, *Socrates: Ironist and Moral Philosopher*, Cambridge University Press, Cambridge.

Watson, D., 2002*, Recollections of a Bleeding Heart: A Portrait of Paul Keating*, Knopf, Sydney.

Watts, R., 2003, 'Making Numbers Count: The Birth of the Census and Racial Government in Victoria, 1835-1840', *Australian Historical Studies*, 2003 , vol. 33, no 118, 33-58.

Whitworth, J. 1998, *Better Health Outcomes Newsletter*, vol 4, no 2 pp. 1-4.

Winter, I., & Seelig, T., 2001, *Housing Research, Policy Relevance and a Housing Imagination in Australia*, unpublished conference paper, presented at 2001 Housing Studies Association Conference, Cardiff University, September.

Young, K., Ashby, D., Annete, B., & Grayson, L., 2002, 'Social Science and the Evidence-based Policy Movement, *Social Policy & Society*, vol 1 no 3, pp. 215-224.

4

Governance and evidence based policy under a national security framework

Marcus Wigan

Professorial Fellow, The University of Melbourne[1]

Abstract

This paper addresses the conflicts of the inherent strains between evidence based policy and contestable evidence based policy under the strictures of a National Security framework. The shifts in attitudes as to what is acceptable in the application of criminal law to civil offences appears to follow the trends set in the Anti-Terrorism Acts. A possible counterweight is improved contestability. It is urged that this issue be investigated carefully in order to ensure better governance in this strained area of civil society.

Keywords: terrorism, threat, contestability, evidence based policy, social informatics, community, accountability, risks, Intellectual Property, ACTA, DCMA, criminalisation

[1] Professorial Fellow in the Department of Civil Engineering, and Partner in the Volvo Centre of Excellence in Transport, GAMUT (Australasian Centre for Governance and Management of Urban Transport) in the Faculty of Architecture of the University of Melbourne.

1 Introduction

The checks and balances in government are always difficult to resolve, and as the complexity of both society and government has increased, the degree to which expertise and policy resides within government has declined. The rise of evidence based approaches to policy in most areas of government has raised the bar for those wishing to gain access and influence with government, in that technically sound and fact based materials now form an essential component of approaches to government.

2 The context

The links between governance and security are usually explored with attention paid more to the risk profile than to the social context. The legal requirement for governance when security is an issue is a subject with a wide and varied basis for discussion, where the assumptions of the enforcement organizations are that their processes are credible, and not usually in terms of human rights and responsibilities.

The sensitivity and availability or otherwise of essential data and information pertaining to specific cases has been an issue of grave concern to the legal profession, due not only to the actual and perceived asymmetries of information and power, but due to the criminalisation of disclosure under the powers of various Anti-Terror Acts (Commonwealth of Australia, 2005).

It is ironic that the seminal case of Roach v Commonwealth Electoral Commissioner (Commonwealth of Australia, 2007) case on voting rights pivots of the severity of the offence involved and the Constitutional powers to withhold the franchise in severe cases. The issue of the freedom to defend oneself with appeal to nondisclosure of pertinent material would normally set the bar for justices so high as to make an appeal to the High Court of Australia. But statute law now appears to effectively make this capacity inaccessible by a combination of clauses in the Acts. Substantial unease over the extreme powers in the Anti-Terror Acts at least partly pertains to the lack of transparency in the administration of justice. Recent events have continued to raise questions, and have made very clear that the organisations such as ASIO and the Australian Federal Police (AFP) (with their very different bases for bringing the law into effect) are now expected to operate at a considerably higher standard of professionalism and trust than other enforcement agencies, due simply to the substantial lack of transparency involved.

The issues of greater trust demanded of the community are closely linked to the higher standards than expected of the agencies. This is not an issue peculiar to Australia, although the US has recently shown that even in the case of those impounded in Guatenamo Bay, that the Supreme Court can call the agencies to account in a manner not yet seen- or perhaps even possible – in Australia.

The social impacts of governance and transparency are considerably wide than such extreme cases, but the necessary inverse links between transparency and professionalism are also applicable to a much wider range of situations than the extreme ones raised in this section.

3 Imbalances in community perception

The central issue (other than the formal issues stated in the previous section) is that information is asymmetric in an increasingly wider range of circumstances. This asymmetry is being exacerbated by the methods by which some organisations have tended to use 'privacy laws' in much the same way that many bodies handle Freedom of Information requests. Governance of privacy itself has attracted attention (Bennet & Raab, 2006) as a pivotal framework for constructive treatment of the inherent conflicts in transparency and accountability with other sensitivities and priorities, private and public.

It is suggested that the inverse link between transparency and the quality expected of the processes within organizations appears to apply equally well to less extreme examples of security, in parallel with the inverse relationships between transparency and power inherent in the privacy area.

All such asymmetries of power are inevitable from a Foucaultian perspective, and such analyses are intrinsic to any examination of governmentality (Burchell et al 1991; Dean, 1999). Bennett et al (2006) emphasise the unclear and multiple policy perspectives that apply to privacy, and thus the divergence between dataveillance (and direct surveillance) and other security tools by different parties with different levels of power. Trust does not figure prominently in Bennett et al, perhaps due to the lesser charge associated with the consequences of failures in National Security, and the greater asymmetries of power and information that have emerged in the latter case.

When privacy of personal data is in conflict with commercial interests, the formal governance tools of data registration, Data Protection Acts (UK, 1998) and other agencies in Australia and in other countries hold the power to act for individual or community concerns. In some cases these powers are weak, or under resourced by Governments. This appears to be the case in Australia in the appointment and resourcing of Privacy Commissioners, and the weak regulatory penalties that they can apply.

Such civil society tools work in accord with the normal perceptions of commercial and tort law and the mechanisms of arbitration, public naming and negotiation with a reasonably well trusted model of operation and dispute resolution that follows.

The difficulty of and individual discovering that his privacy has been breached limits the numbers of complaints to such commissioners, and allows proactive consultation and advice to occur in advance of breaches. However the evidence that privacy breaches have occurred may be pursued by the individual affected to be initiated by the commissioners involved. Trust in the process or the commissioner is not usually an issue.

Once the stakes become higher the fundamental conflicts of executive government and intelligence secrecy upset this delicate balance, and while governance may well be managed reasonably well behind the veils of secrecy, it is far less easy to establish this, or to engender public confidence in situations where:

- The evidence base is not available for review
- The process itself is not transparent
- The external accountability is unclear or absent; and
- The power imbalances are so large and the risks may be commensurately substantial

These risks may be of an entirely different nature and scale to those addressed by privacy principles and processes, but the legal basis for action is also entirely different and founded on different principles, although considerable effort has been expended to make them fit more or less into a similar format as more conventional law, where offences usually have to be committed before legal action is taken.

When intelligence operations are undertaken the goals are to establish a probability of a serious event, and to take pre-emptive action before it occurs. The criminal sanctions that apply are normally the subject of public adversarial legal resolution with strict rules of evidence and disclosure.

In the case of National Security the entire basis of the process bears only a passing procedural resemblance to the conventional public processes of law. The offences are in the main based solely on circumstantial evidence: i.e. indications of a likely situation. Usually no crime has yet been committed, although a range of events have now been criminalized in support of the prospective security mechanisms. Under the Anti-Terror laws now in effect in Australia access to the evidence on which offences are deemed to have occurred (or asserted would probably occur) is strictly quarantined, and asymmetrically available to the two parties.

Similar provisions including long periods to be held without trail or specific charges are now enacted in other countries as well: Australia is hardly unique Furthermore, any legal support is restricted to Government-approved lawyers – and all parties on the defence side are liable to criminal penalties if any discussion is disclosed for up to five years.

This is the antithesis of evidence based approaches to either law or policy, even when the forms might appear to be complied with to at least some degree, the ability to contest such policy or of legal actions is severely limited or specifically excluded, and even ex-post discussion by the parties involved – including the legal practitioners - can trigger criminal charges.

The reliance on evidence remains, but the contestability is largely removed. The application of criminal charges makes this a large step in civil rights.

4 Contestability in policy on the wane

The extreme example of National Security and Anti-Terrorist Acts, is part of a broader social movement which is steadily limiting contestability, and thus reducing the credibility of evidence based policy over a broader front, as the standards both of transparency for criminalisation of behaviour (or prospective expectations of behaviours) and the ability to contest such situation have both shifted substantially. This shift in government and commercial measures to constrain and control social behaviour and strengthen powers (including covert surveillance) appears to be spreading into the civil domain, as the dulled public sensitivity shift induced by the Anti-Terror laws becomes more established.

4.1 A salient example of information asymmetry and dataveillance

The general trend of National Security is to sweep aside many civil rights and reasonable expectations of privacy and fairness and transparency in citizens in their dealings with Government. There is little argument that this is the case, the arguments are more about what level of threat is needed to justify such powers or what triggers should be put in place before activating them, what triggers are needed before activating them, and what levels of accountability (if any) should apply after they have been invoked.

The decisions made by the Government under the National Security banner have already started to infect other areas of government, allowing major asymmetries of power and information, and even criminalisation without *mens rea*. This function creep is an alarming extension of state power, and is **nothing** to do with state security- yet is beginning to display the same sorts of instruments and enabling powers and attitudes in governments (including Australia) without any serious debate on the implications of either the secretive style adopted or the fairly extreme powers in the draft texts in their impact on the community: yet this time it is due simply due to heavy trade pressures from US commercial enterprises.

This novel form of 'function creep' – let us call it 'creeping corrosion of civil society' - is the intellectual property regime imported as a result of the recent US Australia Free Trade Agreement. The Digital Copyright Millennium Act (DCMA) in the US was effectively imported to Australian law – but without the balance of the fair Copying Doctrine that permitted the more onerous impacts on the DCMA on individuals to be contested. Importing the DCMA required criminalisation of intellectual property violation, thus extending the reach of criminal law to almost every person in the country for what are unambiguously civil offences at that level. The massive resources of the IP holders (in most cases very large commercial bodies in the entertainment industry) are thus arrayed against individuals with the threat of a criminal record (now an almost irremovable block on future prospects of an individual) to be invoked for even minor non-commercial deemed violations.

This massive power asymmetry was vigorously contested publicly as this was indeed a matter of public concern, and there are now some limited protections for individuals under Australian copyright law. The lesson? The current round of even more onerous conditions and potentially far more draconian powers are now under negotiation as ACTA (Anti-Counterfeiting Trade Agreement) (Department of Foreign Affairs and Trade, 2007). Once a leak (WikiLeaks, 2007a) of what was being negotiated secretly appeared, the response was very strong. The lack of contestability of this matter is becoming of widespread public concern as much due to the secrecy and lack of transparency (WikiLeaks, 2007b) that it has been progressed. The more extreme comments made about ACTA are balanced to some extent by the cool briefing on the relevant Australian Government website.

This example shows the emergent issues of policy that is non contestable, an the evidence base on which such negotiations are based is also highly polarised between those reporting low levels of violation and those claiming huge losses of revenue. Little of this is well tested and less is fully contestable.

Why raise this here?

ACTA appears to advocate what amounts to full covert surveillance of the Internet in addition to physical inspection, equipment confiscation and criminalisation of the associated at borders. The draft shows that it is intended to operate in a manner that would be hardly contestable, and an even greater imbalance of power between individuals and – this time- the commercial sector using border guards outside their sphere of normal powers.

The convergence of interest between the commercial interests of US copyright owners in exploiting the tools of population dataveillance enabled by Anti-Terrorism Acts is fed by the shift in government attitudes towards what many already regard as unconscionable powers. As is usual with powers enabled beyond reasonable levels, other groups seek to use this new acceptability, and thus the interests of enforcement bodies and commercial enterprises now neatly coincide.

The trend to use criminal rather than civil law for enforcement also has a close parallel with the National Security debate. The lack of contestability of either policy or practice also has the same flavour. It is unlikely that such commercial piggybacking would have been possible to this extent without the shift to secrecy and non-contestability that underpins the Anti-Terror legislation.

The international policy consensus on what comprises appropriate legislative and operational anti-terrorist measures could perhaps have influenced both trade and intellectual property negotiations in the train of the subsequent shared trends towards nontransparency, criminalisation applications, and non-contestability and dataveillance surveillance.

5 Broader considerations

The central issues are those of governance, and evidence based policy – and, we argue, contestability. Some of the cross overs between these concepts and National Security issues and perceptions resulting from national and international moves to address National Security goals have been discussed here, but the issues are of course broader, and apply considerably more widely. We will consider two (relatively) uncontroversial cases, one international and one national.

A common issue in policy is that a range of different technical argument, based on very different types of data and evidence, has to be brought to bear on a single course of policy action. If this range of inputs is not reduced to a much smaller set, then policy is very difficult to resolve technically, let alone politically. Consequently there is always pressure to limit the scope of any such technically based materials for policy crystallisation. The results can often be a lack of transparency – but not due to the lack of the reports of the evidence, more in the range of options pruned before disclosure.

This can lead to over simplistic policy, a finding of a wide range of studies done across the world by Crewe and Young (2002) where the information and simplified research or technical outputs were not contestable – and even used to rationalise flawed polices. Contestability is therefore central to addressing this flaw in evidence-based policy. The enthusiasm for evidence based policy in the UK has been the context of performance measures for all aspects of government, a limited form of contestability, but is criticised for the instrumental rationality approach that it has engendered (Sanderson, 2002). No comment is made by either author on the selective use of either studies or performance measures to intentionally limit contestability to achieve less than ideal policies!

Another example, a little more controversial, is the consultation process for the Eddington Report on East West Link Need Assessment (Department of Infrastructure, 2008) in Melbourne. Here a carefully circumscribed region is analysed, not using the Government Models for Melbourne, but a different commercial one, and no access to this model was made possible. This is a rather different example of lack of contestability, where the framing of the study reports effectively precludes a contestable process. Harding (2008) succinctly summarises this process as follows:

> "Experience with evidence-based policymaking in Britain raises doubts about such claims. The British experience led to the term "policy-based evidence", to describe the end result where government agencies filtered out information that was inconsistent with government policy".

These two examples are simply to illustrate that the processes of evidence-based policy still require contestability, whether or not National Security is an issue.

6 Conclusion

The links between governance, evidence based policy and practice are insufficient for the sound operation of National Security, and require a measure of contestability. This conclusion applies equally well to the areas of National Security and those of broader governance.

The central measure of social impact is the trust of those empowered to undertake the governance of these processes, a trust that is difficult to establish and in the case of National Security has been shaken by the manner in which a series of Anti-Terror prosecutions have been handled in the last few years. The less transparent the process, the more that internal and non-contestable governance is used, the greater the degree of community trust that is needed.

It is hard to beat the simple statement of the UK Standards Board (Accessed

2008).

> "At the heart of good ... democracy is a bond of trust between the community and the people who represent them – a bond which depends greatly on the conduct of those people.The public have a right to expect the highest standards of behaviour from their representatives and those responsible for the delivery of ... public services".

These sentiments apply generally for governance, and never more than when the confluence of intelligence and security invokes surveillance and pre emptive action in the community interest: the move to expect similar powers in support of commercial interests is an unwelcome extension, where the preconditions of trust are harder to establish and even harder to maintain.

The privacy issues involved in dataveillance are widely discussed (K & MG Michael, 2006, 2007), but the extension of the contestability principle to National Security is an issue that requires careful review of the privacy principles, as the issues are in some tension. But good governance and trust may yet make it necessary.

It would be timely to reassess the manner in which trade agreements are now beginning to reflect the precedents for official attitudes towards their own citizens arising from the very different context of intelligence powers. This is peculiarly pertinent in Australia, which has no Constitutional powers formally equivalent to a Bill of Rights· Although implied rights are slowly being deduced by the High Court, this is necessarily a highly restricted, slow, and incremental process also restrained by the limited coverage of many modern issues in the Australian Constitution – whereas the US has contestability in its Constitution, and it is being exercised. Non US citizens have no such protection.

Greater contestability is highly desirable. How – and even if - this is to be achieved is very uncertain, but demands early attention in the interests of all, including National Security and its community support.

References

CJ Bennett & Raab, CD. 2006 *The governance of privacy – policy instruments in global perspective*, MIT Press, Cambridge MA.

B. Burchell, Gordon, G & Miller, P. [Eds] 1991 *The Foucault effect: Studies in governmentality with two lectures and an interview with Michael Foucault*. University of Chicago Press.

Commonwealth of Australia. 2005. Anti-Terrorism Act 2005 No 127, 2005 An act to amend the law relating to terrorist acts, and for other purposes: at http://www.comlaw.gov.au accessed 22 June 2008. Also a compendium of relevant law and related Acts at http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D49EA90CA256FAB001BA5EA?OpenDocument accessed 30 June 2008.

E Crewe & Young, J. 2002. *Bridging research and policy: Context, evidence and links*. Working Paper 173, Overseas Development Institute, London.

M. Dean. 1999. *Governmentality: Power and rule in modern society*. Sage, London.

K & MG Michael, 2005 [Eds]. '*The social implications of information security measures on citizens and business : The first workshop on the social implications of National Security'*. University of Wollongong Press.

K & MG Michael, 2007 [Eds]. '*From dataveillance to Uberveillance and the realpolitik of the transparent society: Second workshop of the social implications of National Security 29 October 2007'*. University of Wollongong Press.

Commonwealth of Australia. 2007. *Roach V Electoral Commissioner (2007) ALR 2399.*

Department of Foreign Affairs and Trade, 2007. At http://www.dfat.gov.au/trade/acta/index.html accessed 30 June 2008.

Department of Infrastructure, 2008. At www.doi.vic.gov.au/Doi/Internet/planningprojects.nsf/ accessed 30 June 2008.

D. Harding, 2008. '*FuelWatch evidence runs on empty'*. The Age, Melbourne 2 July at http://business.theage.com.au/fuelwatch-evidence-runs-on-empty-20080701-3045.html?page=1 accessed 2 July 2008.

I. Sanderson, 2002 Making sense of 'What works': Evidence based policy making as instrumental rationality? *Public Policy and Administration* 17(3), 61-75.

UK Data Protection Act, 1998. At http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1. Accessed 1 July 2008.

UK Standards Board www.standardsboard.co.uk, accessed 30 June 2008; also quoted by Bennett and Raab (2006).

WikiLeaks, 2007a. At wikileaks.org/leak/acta-proposal-2007.pdf accessed 30 June 2008.

WikiLeaks, 2007b.
http://wikileaks.org.uk/wiki/ACTA_trade_agreement_negotiation_lacks_transparency is illustrative of the results of undue secrecy accessed 30 June 2008.

5

The risk intelligence conundrum and its impact on governance

Mark Loves

Senior Lecturer, Program Manager, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

This paper looks at intelligence led strategic planning, specifically within the context of an operational private sector corporate security unit which the author managed from 1994 to 2005. It examines the role, mission and objectives of the unit, with specific emphasis on management models, planning frameworks, policy and strategy, client relations and performance measuring. It develops the concept that risk assessment and intelligence development are in fact the same process, acting to direct governance and informing decision making at both tactical and strategic levels.

Keywords: intelligence, strategic planning, compliance, risk management, risk intelligence, value chain model, value network model, value workshop model, internal consultancy model, client relations, performance measurement

1 Introduction

In any paper on intelligence, it becomes necessary to define the term, as there is the potential for confusion surrounding its meaning. Intelligence, as it is applied in a national security context is a process, defined by its components which are popularly categorised as planning, collection, collation, analysis and dissemination. However the term intelligence is also used to describe the end product of that process, as well as defining organisations or groups that carry out the various functions involved in the process (Lowenthal, 2006). For the purpose of this paper, intelligence is defined by its process, which is designed to add value to information and ultimately focused on assisting policy makers in their decision making.

Within traditional law enforcement and national security, intelligence has traditionally been regarded as an operational, strategic or tactical driver. However, with ever increasing demands on organisational efficiency and effectiveness, intelligence is now being promoted as a formal basis for strategic business planning (Christopher, 2004). In this context the intelligence function or what intelligence is used for, involves the proactive interpretation of the business environment. It has at its core the ability to respond flexibly to situations, to manage risks, take advantage of fortuitous developments, make sense of contradictory information and ensure efficient and effective results from operations and strategies (Grieve, 2004). Ultimately, intelligence is used to inform decision making at the tactical and strategic levels and is designed to act as a guide to managing operations (Ratcliffe, 2004).

In contrast, traditionally risk has been used to describe the chance of something happening that will impact upon the achievement of organisational objectives. Risk assessment as a process, is based on a measurement of impact and probability. It derives from notions of capitalism, religious turmoil and scientific vigour born of the French Renaissance period, when probability theory was transformed from a "gamblers toy" to a method of predicting and benefiting from the future based on the organisation, analysis and interpretation of available information. This transformation is described by Bernstein as the beginning of the theory of decision making, "deciding what to do when it is uncertain what will happen" (Bernstein, 1998). Upon consideration, this mix of limited information, uncertainty and decision making bears startling similarity with the intelligence process and functions.

This paper looks at the issue of strategic planning within the context of an operational private sector corporate security unit and examines how the role, mission and objectives of the unit drive the development of strategy and policy through risk assessment. It also examines similarities within the disciplines of risk and intelligence and draws conclusion on their interdependence within an overarching framework of governance modelling.

2 Management model

Management is regarded as the process of coordinating work activities so that they are completed with and through other people, in the most efficient, "doing things right" and effective, "doing the right things" way (Robbins, Bergman, Stagg & Coulter, 2006). Whilst there are numerous management models, consensus is that they are generally derivations on three critical management functions; planning, (defining goals, establishing strategy and developing plans), organising (arranging work to accomplish goals) and controlling (evaluating whether things are going as planned) (Robbins et al. 2006; Rogers, Ure & Young, 2007; Stoner, Collins and Yetton, 1985).

In strategic planning, intelligence is critical in assessing client expectations and selecting which management model is best suited to the role, mission and objectives of the unit. Intelligence also impacts upon management modelling, as it can provide performance feedback which may reflect on the adequacy of the model. Intelligence therefore can act as a catalyst for change or amendment to the management model.

2.1 Role, Mission and Objectives

Within the corporate security unit, the role, mission and objectives were established at the planning stage of the management model (diagram 2), although they had real implications for both the organising and controlling stages. The unit's role was to support the company in achieving its corporate objectives, being the maintenance of profitable operations through effective utilisation of its critical infrastructure and resources. Its mission was the identification and protection of those critical assets and infrastructure most responsible for assisting the company achieve its corporate objectives. The unit's objectives related to the efficient and effective establishment and implementation of infrastructure, physical asset, information (logical, intellectual and hard copy), personnel and financial security risk plans, to protect the assets thus identified and to provide business continuity in the case of catastrophic loss (Broder, 2000). To achieve these objectives, the author devised and implemented the management model (diagram 1), which also acted as a governance framework.

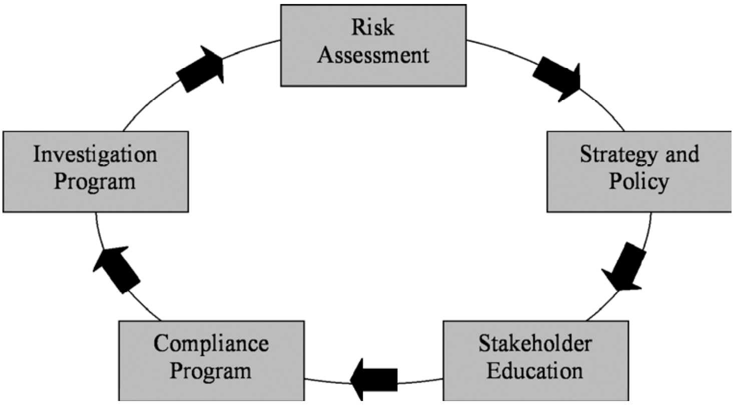


Diagram 1. Corporate Security Unit risk based governance framework

3 Management planning framework

Rogers et al. (2007) describe several models within management planning frameworks. The Value Chain Model describes the process of producing consumer goods from raw materials. The Value Network Model matches client needs with services offered, to mutual advantage. The Value Workshop Model involves the client being treated as the focus of attention, where the only identifiable output is the client's satisfaction. Finally, the Internal Consultancy Model focuses on delivering products and services that can't be obtained elsewhere.

In the author's experience within policing, security and intelligence agencies, the Value Workshop and Consultancy Models were predominantly utilised. Within the corporate security unit, a similar consultative risk based management planning framework was utilised [diagram 1], involving risk assessment, developing policies and strategies to address unacceptable risks, education programs, (to educate decision makers and other stakeholders on those risks, strategies and policies), compliance programs (to ensure stakeholder implementation), and where control failures were identified, investigative programs to identify cause and develop remedy. This whole process then fed back into the risk assessment phase and the model would commence again.

Intelligence considerations played a dominant role in the development of this framework with its major emphasis on risk assessment (intelligence development) as the core of the management model. To demonstrate the risk/intelligence relationship, the author developed comparative modelling to demonstrate to the company (client) how intelligence overlaid the risk management process (diagram 2). In this model, the risk management and intelligence functions are complementary, if not the same process however, it's not so much the governance framework contributing to the intelligence function as it is the intelligence function driving the framework. Apgar (2008) describes a similar process in using the example of telecommunications company AT&T, in observing that the company's inability to understand its capacity for taking risks led to a too cautious approach to the introduction of broadband Internet services in the 1990's, a policy decision which ultimately led to its financial detriment. In this context, he interprets risk intelligence as "our ability compared to competitors to assess a risk".

The first step in the management planning framework was a consultative organisational security risk assessment (diagram 1). This assessment was initially conducted as a series of site visits, observations and interviews with internal and external stakeholders (including senior executives). Information was also gathered from industry benchmarks, statistical incident and insurance data bases, agency reports, internal / external audit and industry experts. Comparative analysis was then conducted across the information to develop risk intelligence. The aim of this risk intelligence process was to:

- identify those assets, personnel, information, processes and systems (including financial) which were most critical to the Company in achieving its corporate

objectives,
- identify the major security risks to those critical assets, and
- assist in identifying potential policy and strategy that would assist in protecting those critical assets.

The model met three major criteria for the successful use and management of intelligence within organisations (Rogers, et al. 2007). It provided an upward organisational focus (risk assessment, policy and strategy) where intelligence was emphasized as a means for achieving the goals of the company. It provided a downward focus to ensure that these organisational priorities were understood and implemented by the work force (education and compliance) and it provided a facility to identify and address issues and non performance at an early stage ("focus on self") at the investigation phase.

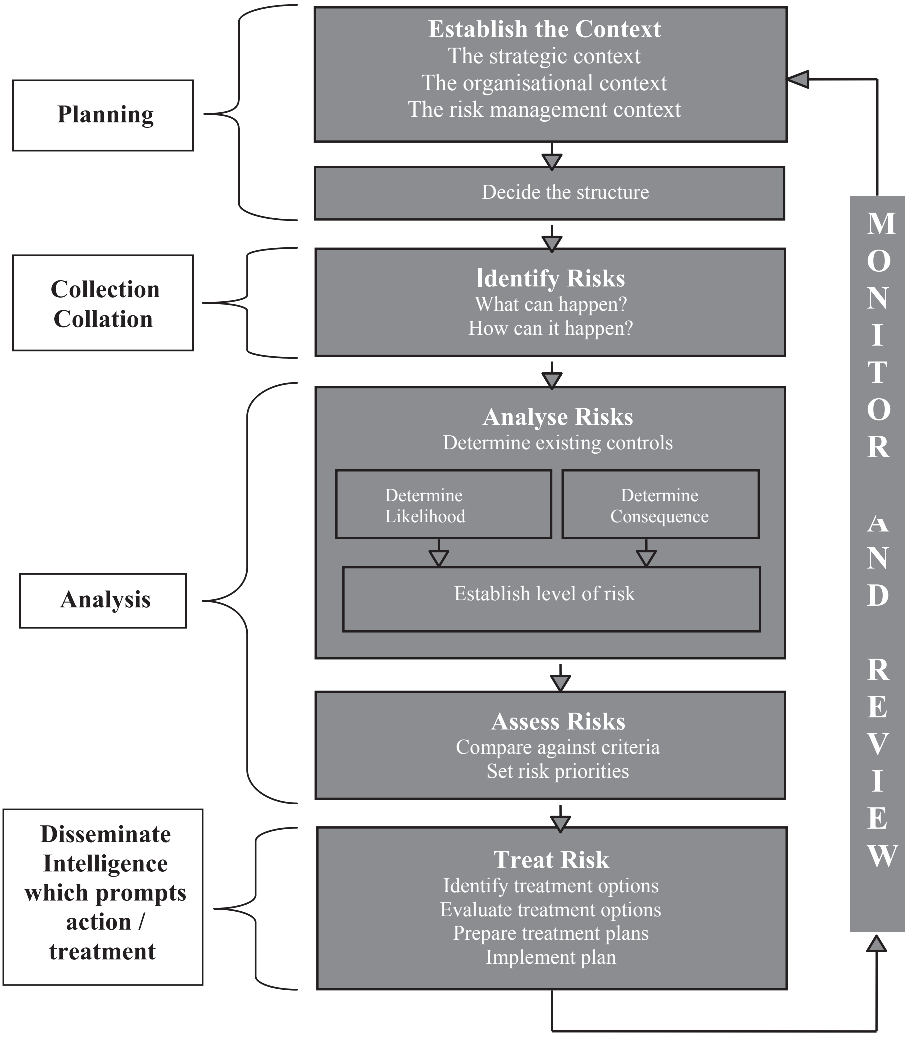


Diagram 2. The relationship between intelligence and risk management
(Based on AS/NZS 4360:2000 - Risk Management) – (Loves, 2000)

4 Policy and strategy

There appears to be no universally accepted definition of strategy. Mintzberg and Quinn (1991) described it as a pattern, ploy, plan or position that integrates organisational goals into a cohesive whole, which deals with the "*unpredictable and unknowable*". Maister (1997) described strategy as finding new ways to do things, or an improvement in core business requiring changes in behaviour. Yarger (n.d.) agrees that strategy is a general plan or course of action which is both proactive and anticipatory, but goes further to describe it as hierarchical (cascading from top level down), comprehensive (considers the whole of the strategic environment) and developed through analysis. Yarger describes risk as inherent in all strategy and *"the best anyone can do to offer favourable balance against failure."*

The concept of strategy adopted by the corporate security unit drew on a combination of these. Strategy is best described as a "proactive, anticipatory and comprehensive risk based plan of action to address and manage unacceptable risk identified in phase one of the management model" (diagram 1). If it is accepted (as asserted earlier in this paper) that the risk and intelligence processes are complementary (if not the same process), then it can be said that intelligence was the driver of strategy within the corporate security unit.

Within the unit, management was aimed at achieving objectives through people, and strategy became the broader plan to achieve those objectives through changing behaviour (Maister, 1997). Policies became the resultant rules and guidelines that set limits for action and guided the behaviour of the personnel within the unit, and within the organisation (Mintzberg et al. 1991).

With intelligence considered as the driver of strategy within the corporate security unit, and with strategy focused on "ends" (achieving corporate objectives), then policy became the "means" to achieving those ends, through controlling unit and organisational employee behaviour. Policy, therefore can be said to have dominated strategy through an *"articulation of the end state and its guidance"* (Yarger, n.d.).

Hence policy could be considered a derivative of the same intelligence used to drive strategy within the unit (risk assessment). Intelligence was also used after implementation of the policy, to obtain feedback from stakeholders (executive, coal face staff, and internal/external audit), monitor whether it was actually achieving the objectives of the strategy or whether the policies (and indeed strategy) required change or amendment.

The ultimate value of intelligence is to guide policy makers in their decision making (Lowenthal 2006). In the model (diagram 1), risk assessment was used to provide the policymakers with information to best address the critical risks facing the business. That is not to say that the policy makers did not have input at the risk assessment stage. Strategic planning provided opportunity for policy makers to influence and shape the intelligence upon which their decisions were based. Ultimately it was that intelligence that provided the basis for decision making and ultimately supporting governance through, " doing the right things, in the right way, for the right people, in a timely inclusive, open, honest and accountable manner" (CIPFA, 2008).

5 Client relationships

Managing client relationships and ensuring client satisfaction is critical for any organisation or business unit. Rogers et al. (2007) described the client as the "beginning and the end", whilst Hartley (1994) observes that the ultimate test of an intelligence based product is client acceptance and whether any significant policy maker takes notice of the risk/intelligence assessment and changes policy. The value workshop model utilised at the corporate security unit had at its core a focus on the client. The unit also utilised elements of the internal consultancy model which focused on independence, security specialisation and upon delivery of expertise that can't be obtained by the client elsewhere.

The difficulty for the unit was often deciding exactly who its clients were and in prioritising service to them. Given the broad application of its services, the unit's client base varied to include company executives, shareholders, employees and customers, depending on the context of the service application. Corporate security and its associated intelligence products drew such a broad brush across both the strategic and tactical levels of the business that the unit often had to split its focus on delivery of services with resultant difficulties in resourcing and balancing competing interests of clients. Prioritisation occurred where risks were greatest, and this was normally based on criticality. Through communicative and consultative processes, the unit was able to build up an excellent strategic picture of the client's business, recognise and prioritise demands from competing and multiple clients, and manage the client's expectations.

Within the risk context, intelligence was heavily relied upon to provide a support function for critical asset protection. Major difficulties were often experienced through the client having unrealistic expectations of the time and effort involved in developing such intelligence, the difficulty in obtaining the necessary information, and the specialist skills required to support intelligence development (Ratcliffe, 2004). Client education, particularly at executive levels, communication and listening provided the solution to this problem by ensuring that the client and the unit had the same notion of task and desired outcome, particularly at strategy level. The corporate security unit first had to identify the multiple risk based services required by the client and then ensure that the programs developed met the expectations of the client, whilst at the same time ensuring that prioritisation was utilised to maximise the use of finite resources within the unit (Rogers, 1988).

Intelligence was utilised within the security unit as part of a systematic structured program of management, not only to obtain information regarding projects, tasks to be performed, skills required and time frames expected, but also to ascertain client preferences and priorities, challenge competing strategic goals, making sound strategic trade offs, tracking project time and costs, unit productivity and work quality (Maister 1997). Intelligence was also useful in assessing client satisfaction through feedback, thereby allowing the opportunity to improve service and build client relationships and confidence in the services provided by the unit. Intelligence facilitated ongoing direction, redirection and focus during projects and provided the mechanism for review and feedback post project. Ultimately, it provided a basis upon which to establish a *"security management institution"* where inclusive risk orientated considerations and arrangements became part of highly institutionalised managerial practice (Haftendorn, Keohane and Wallander, 1999)

6 Measuring performance

If two of the critical issues impacting upon client relationships are a focus or concern on the clients needs and how useful the intelligence was to the client and whether a significant decision maker used the intelligence to change policy, then the key to achieving these outcomes was feedback, continuous improvement and refinement of the intelligence processes to deliver progress towards achieving the corporate mission and objectives. This can only be achieved through measuring the performance of stakeholder groups within the organisation (Hartley, 1994).

Any management plan is incomplete without reliable and objective measurement criteria to assess effectiveness, efficiency and quality of service. Rogers (1998) compares performance measurement with the nautical concept of taking sextant readings. Like its nautical cousin, performance measurement provides an indicator of whether the management program is on course. Within the management planning framework adopted by the corporate security unit (diagram 1), the compliance and investigation phases were used to measure performance and provide for continuous improvement. Compliance programs were used to ensure that the policy and strategy devised as a result of the risk assessments were being implemented, and that managers were *practicing what they were preaching*. Where control failures were detected, investigations were instigated to identify the cause and implement improvements.

Three major benefits arose from implementing effective performance management and measuring processes. The first was the unit's ability to evaluate its performance (in using intelligence) in assisting the development of strategy and policy to protect critical company infrastructure and assets. Next, it allowed the unit to monitor the activities of those charged with responsibility for implementing the strategies and policies, providing an early alert system to control failure and opportunity for remedial action. Finally, it allowed the corporate security unit and stakeholder managers to learn from experience to change or improve processes to enhance progress towards, and achievement of objectives.

There were a number of possible causes of control failure within the model. The strategy or policy may well have been based upon flawed intelligence (risk assessment) or alternatively, the failure might be due to non compliance of individual managers. Irrespective, these issues would be identified at the investigation phase and fed back into the risk assessment phase in a repeating circular process, thereby facilitating continuous improvement.

Intelligence played a critical role in the evaluation and measurement of performance by proactively providing insight into whether strategy and policy were working, and whether they were being effectively implemented by key stakeholders. It provided useful focus upon the areas most at risk and concentrated resources where they were most needed, thereby providing for accountability at both the stakeholder and security unit levels (Woodhouse, 1997).

7 Conclusion

Ultimately, the usefulness of intelligence in the context of strategic planning is in providing plans, oversight, guidance and direction. It links performance with the management processes. It enables managers of work units to make informed business decisions. It improves the timeliness and quality of those decisions, enhances communications with clients and stakeholders and measures satisfaction, thereby improving client experience. It ensures available information is directed and targeted towards achievements of objectives and identifies and addresses barriers and unacceptable risks to the business, thereby supporting corporate governance at multiple levels of the organisation.

The management planning frameworks adopted by the corporate security unit were the *Value Workshop* and *Consultancy* models, which drew heavily upon establishing client relationships and ensuring client satisfaction with the services provided. Within the context of the corporate security unit, risk assessment was critical not only in its context as a phase of the management model, but also in *identifying client's needs, wants and ultimately, satisfaction.* Policy and strategy were developed to address unacceptable risks and intelligence was then employed to not only ensure adequacy of, and compliance with policy and strategy, but to also measure progress towards objectives. The model demonstrated how risk assessment can be used to drive corporate strategy and ensure appropriate governance.

This paper looked at a management model implemented for a private sector corporate security unit (diagram 1). The intelligence function and risk assessment have been identified as essential elements of the model. The model has risk assessment at its core, a function that has been compared and overlaid with the intelligence process (diagram 2), to conclude that they are the same processes, supporting the notion of the convergence of intelligence and risk within a corporate context.

References

Apgar, D (2008) Increasing Risk Intelligence – How does your company manage risk? Retrieved 19/6/08 from http://www.businessweek.com/print/innovate/content/aug2006/id20060818_495984.htm

Australian and New Zealand Standard 4360:2000 - Risk Management

Bernstein, P.L. (1998) 'Against the Gods, the remarkable story of risk,' John Wiley and Sons. New York, pp 3 - 69.

Broder, J.F. (2000). Risk Analysis and the Security Survey, 2nd edition. Butterworth Heinman, Boston, p 139.

(CIPFA) Chartered Institute of Public Finance and Accountancy UK 2008, Improvement network. 'Governance, what is it about.' Retrieved 2/6/08 from http://www.improvementnetwork.gov.uk/imp/core/page.do?pageId=1007044

Christopher, S. (2004) A practitioner's perspective of UK strategic intelligence. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press, Australia, p 177.

Grieve, J. (2004) Developments in UK criminal intelligence, in Strategic Thinking. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press, Australia, p 25.

Hartley, J 1994, 'Concluding remarks', in Intelligence and Australia's National Security, A Bergin & R Hall (eds) Australian Defence Studies Centre, Canberra, pp 171-175.

Hewlett Packard (2007) 'Risk Intelligence Architecture – converting information to intelligence (White Paper), p3. Retrieved 15/5/08 from http://h20219.www2.hp.com/ERC/downloads/4AA1-5361ENW.pdf

Haftendorn, H. Keohane, R.O. & Wallander C.A. Imperfect Unions, Oxford University Press 1999, p 12.

Loves, M. (2000) *Fraud Intelligence Processing Systems* (Study Unit 8), Diploma in Fraud Management and Certificate in Fraud Control, Australian Centre for Security Research, University of Western Sydney, Macarthur, p 3.

Lowenthal, M.M. (2006) 'Intelligence, from secrets to policy, 3rd edn.' CQ press, Washington, p 9 - 174.

Maister, D.H., (1997). *Managing the professional service firm*. New York, Free Press, pp 179 – 224.

Mintzberg, H. & Quinn, J.B. (1991). The strategy concept, in *The strategy process: Concepts, contexts and cases.* 2nd Edn, Prentice Hall, Englewood Cliffs, NJ, pp 3-20.

Ratcliffe J.H. (2004) The Structure of strategic thinking. In, Ratcliffe, J. (ed), Strategic Thinking in Criminal Intelligence, The Federation Press, Australia, pp 8 – 55.

Robbins, S, Bergman, R, Stagg, I & Coulter, M. (2006) 'What is management?' and 'What do managers do?', in Management, 4th edn, Prentice Hall, Sydney Australia, pp 4 -18.

Rogers K (1998), Evaluating strategic intelligence assessments: some sextant readings for law enforcement', Journal of the Australian Institute of Professional Intelligence Officers, vol.7, no.3, pp 23-94.

Rogers, K., Ure, J., & Young, L.J. (2007). *Intelligence Management,* Bathurst, Charles Sturt University. pp 3-11.

Stoner, J.A.F., Collins, R.R., & Yetton, P.W. (1985). Management in Australia, Sydney, Prentice-Hall, pp 16 – 128.

Woodhouse M 1997, Intelligence driven policing – A United Kingdom model' Journal of the Australian Institute of Professional Intelligence Officers, vol 6, no. 2, pp 49-111.

Yarger H.R. Towards a Theory of Strategy: Art Lykke and the Army War College Strategy Model. Retrieved 29/9/07 from http://dde.carlisle.army.mil/authors/stratpap.htm

6

Policy implications of convergence in the new security environment: An investigation into the symbiosis between risk management and intelligence

Katina Michael[1] and Mark Loves[2]

[1]Senior Lecturer, School of Information Systems and Technology, University of Wollongong, [2]Senior Lecturer, Program Manager, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

For some time there has been a movement away from the traditional view of security as a purely functional activity which occurs within a single department of an agency or enterprise, to security being understood as a value added capability serving the overall mission of an organization. Enterprise risk management (ERM) is a process that is conducted by private companies for the purpose of due diligence informing key decision makers like chief information officers (CIOs). In the same light, the intelligence cycle is conducted by government organizations for the purpose of maintaining national security and informing policy makers like heads of state, ministers and other agencies tasked with security such as the military. The new security paradigm has spurred on the development of enabling business processes that have not only an enterprise-wide view of risk but an interdependent organization-to-organization view of risk. Entities interconnected in the intelligence community (IC) must consider sharing their information to ensure robustness in their decision-making capabilities. In changing the way things have been done, entities in the new security environment are undergoing the trend of convergence on a number of levels including information, products and services, platforms (i.e. standards), and organizations. Of importance in this paper, is the convergence and integration occurring between the risk management and intelligence cycles which has born about the emerging concept of risk intelligence (RI).

Keywords: Security convergence, enterprise risk management, intelligence cycle, real-time business intelligence, risk intelligence

1 Introduction

This paper argues that convergence is occurring within the security environment, notably in the disciplines of intelligence and risk management. Commentators are unanimous in their assessment that the security environment is undergoing a steep rate of change in the way the intelligence community functions, some stating that the change is so dramatic that it can even be considered revolutionary. The trend of convergence is prevalent at multiple levels, causing a cultural shift[1] away from a silo and stovepipe mentality towards transparent information sharing. The paper begins by defining convergence in the new security environment, and broadly outlines the different types of convergence that have been defined in the literature. A normative description of risk management and intelligence is then provided, showing the basic steps carried out for each by enterprise and government organizations. The contribution of this paper is in identifying how risk management and intelligence cycles can be integrated through business processes and the benefits ensuing from this integration. Beyond integration, it is predicted in this paper that the risk management and intelligence processes will soon be referred to interchangeably and universally in the literature. The emerging concept of "risk intelligence", explicitly merging together the domains of 'risk management' and 'intelligence' is then discussed prior to concluding remarks restating the importance of the trend of convergence in the new security environment.

2 Security convergence

The term "convergence" has its roots in mathematics and the natural sciences dating back to the late sixteenth century.[2] In its modern interpretation "convergence" has to do with the evolutionary trends in technological development.[3] The term is therefore now linked to the idea of symbiosis occurring between products or between processes.[4] At an enterprise level, convergence can be observed as individual business units come together to enhance security for the purpose of creating competitive

[1] United States Government Accountability Office, 'Information Security Management' (U.S. Government, 1998) 28. '… it is likely a "cultural shift" will occur among the public safety agencies, organizations and personnel. This "cultural shift" is more a product of the process than an intended consequence. The SMEs in a recent panel stated: "As a consequence of the collaboration, information sharing, and coordinated activities inherent in adopting and executing a Risk Management Model, or some other analytical risk and vulnerability model, it is expected that there will be a "Cultural Shift" in the public safety community.'

[2] Edward P. Borodzicz, *Risk, Crisis and Security Management* (2005) 13.

[3] K. Michael et al, 'The hybridization of automatic identification techniques in mass market applications: towards a model of coexistence' (Paper presented at the Third International Conference on Management of Innovation and Technology, Singapore, 21st–23rd June 2006) 1046.

[4] Katina Michael, 'Trends in the selection of automatic identification technology in electronic commerce applications' in N. Cerpa and P. Bro (eds), *Building society through e-commerce: e-Government, e-Business and e-Learning* (2003) 135.

advantage.[5] At a state level, convergence can be understood within the context of national security, as agencies that start looking more and more alike come together to engage in collaborative efforts to meet performance criteria, and to ultimately reduce costs by removing duplication and redundancy. ASIS International defines "security convergence" as:

> 'the identification of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies.'[6]

A more recent definition of security convergence states its relevance to enterprise security risk management (ESRM)[7] and emphasizes the combined management of physical and logical security.

2.1 Types of security convergence

In discussing convergence, this paper engages the reader at four different levels (figure 1):

- Convergence of *security organizations* at the national and enterprise level.[8] This type of convergence includes companies that are coming together to offer solutions to the intelligence community, as well as convergence of government agencies that would work more effectively together than as stand-alone organizations;
- Convergence of *security processes* (i.e. standards/ platforms). This involves the identification 'of security risks and interdependencies between business functions and processes within the enterprise and the development of managed business process solutions to address those risks and interdependencies';[9]
- Convergence of *security products and services*, fundamentally involving 'different companies' people and IT systems working together to deliver a convergent

[5] Allen Booz, *Convergence of Enterprise Security Organizations* (8 November 2005) The Alliance for Enterprise Security Risk Management <www.asisonline.org/newsroom/alliance.pdf> at 1 May 2008 6.

[6] Ibid 4.

[7] Michael P. Johnson and Jeff M. Spivey, 'ERM and the Security Profession' (2008) 55(1) *Risk Management* 31. 'ESRM is a holistic risk management process that aligns organizational drivers affecting strategy, processes, people, technology and knowledge to protect key assets in accordance with governance, risk, and compliance (GRC) requirements. ESRM requires cross-functional collaboration within the back drop of ERM between multiple management disciplines including, but not limited to physical and logical security, safety, legal, risk management, crisis management and business continuity planning.'

[8] Jagdish Pathak, 'Risk management, internal controls and organizational vulnerabilities' (2005) 20(6) *Managerial Auditing Journal* 569.

[9] Michael Peterson, *Information Convergence, Transforming the Information-Centric Enterprise* (2006) SNIA Data Management Forum <www.sresearch.com/articles/SRC-DMF-Article_Information-Convergence_20060112.pdf > at 27 April 2008 3.

product or service';[10] and

- Convergence of *information*, ie sources and quality content that is used to inform business processes, including technical, human, open source intelligence etc.[11]

The model of convergence has been said to be 'ideal' for 'managing uncorrelated... risk through a systematic, coordinated process.'[12] However, the complexity of convergence in reality should not be understated.[13] Taking policies and processes that were once created in silos and trying to make some collective sense out of them to institute change, is multifaceted and complicated.[14] While at the enterprise level convergence is being driven by compliance,[15] government agencies and organizations have not come under similar scrutiny.

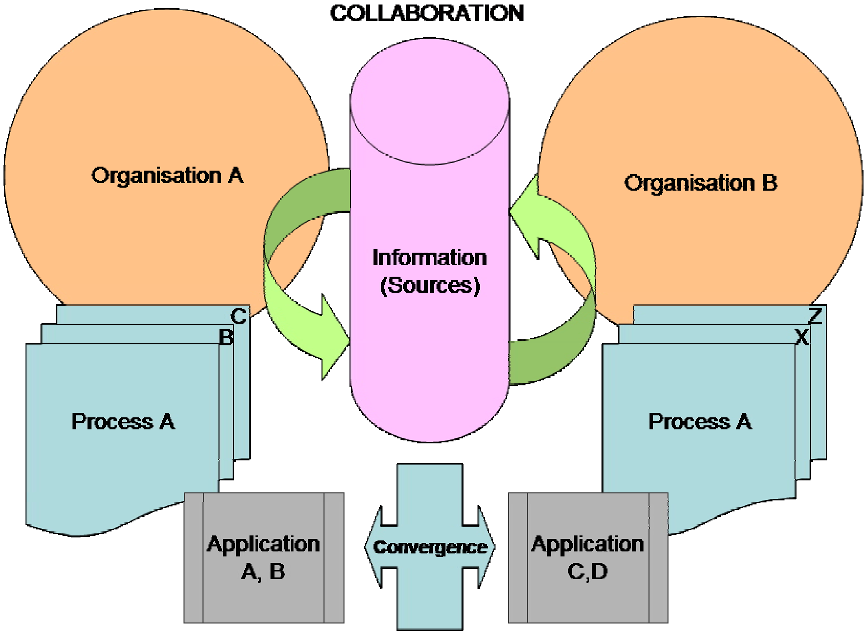


Figure 1. Convergence in the new security environment

[10] Mark Layton, *Urgent Convergence: Fostering Risk Intelligence in the Technology, Media & Telecommunications Industries* (2008) Deloitte <www.deloittte.com/RiskIntelligence> at 27 April 2008 2.

[11] Peterson, above 9, 3.

[12] Todd L. Williams, 'Convergence' (1999) 46(8) *Risk Management* 14.

[13] Margaret T. Wrightson and Stephen L. Caldwell, 'Risk Management' (United States Government Accountability Office, 2005) 8. 'The task of managing this complexity centers on the Department of Homeland Security, which since its inception in March 2003 has been faced with the challenge of transforming 22 agencies into an organization that can plan, manage, and carry out operations effectively.'

[14] Matt Podowitz and Brian Tretick, *Compliance, Convergence and How IT Fits* (8 January 2008) CIO <http://www.cio.com/article/print/170000> at 27 April 2008 1.

[15] Ibid 1.

2.2 Security as a value add

The premise for the convergence phenomenon sweeping the global security industry has been a shift in mindset that sees security as a "value add" to the overall mission of businesses and government agencies alike.[16] It is the realization that security cannot be achieved alone, but requires a meshed network of stakeholders and entities to work together towards a common goal. More than any other event in recent U.S. history, September 11 (2001) showed the failure of intelligence agencies in sharing information regarding possible terrorist targets. For instance, an inquiry into the actions of the Federal Bureau of Investigation (FBI) concluded that the main problems were: severely inadequate information and communication technology (ICT) systems, an inability to bridge together human intelligence (HUMINT) and technical intelligence (TECHINT) to conduct all source analysis, and problems related to the recruitment and training of analysts.[17] Apart from asymmetric terrorist strikes that have caused significant loss of life post September 11, imperatives towards convergence in the security environment have come from enabling high technologies that have blurred traditional functional boundaries, new compliance and regulatory regimes, and the emphasis today on information-based assets (i.e. as opposed to physical items).[18] Security convergence has meant change in the context of:

- *people* and their respective roles and responsibilities;
- *processes* in terms of standards to follow and regulations; and
- *technology* in terms of enabling tools and applications.

2.3 The end-to-end security lifecycle

The motivation behind convergence in the security environment is one that espouses a whole-of-life,[19] holistic,[20] highly collaborative exchange between organizations and agencies. It is a movement away from the silo functional organizational security view which treated the areas of prevention, detection, response and recovery separately, toward a view which espouses the entire end-to-end security lifecycle as a super-system. The challenge with such a system is getting organizations and agencies who have thought and acted a particular way for decades, to change their ways and to begin working closer together in order to

[16] Booz, above 5, 4.

[17] Peter Gill, 'Intelligence and the Post 9/11 Shift' (2004) 19(3) *Intelligence and National Security* 467–489 475.

[18] Booz, above 5, 8.

[19] Russ Banham, 'The convergence of risk' (1995) 42(7) *Risk Management* 22. 'Companies that regard all their risks as a totality can better make decisions to protect themselves from risk.'

[20] Ibid 23. 'Academically the concept of holistic risk management seems to represent an effective risk management strategy.' See also, Podowitz and Tretick, above 14, 1, who call this a 'federated' approach.

solve problems.[21]

The *new* security environment[22] is characterized by strategic changes, changes to processes, and changes to the roles and responsibilities of people in security organizations. The nine traditional operating levers can be adapted to help organizations perform better in the new converged security environment. The levers that can be applied with respect to internal and external drivers include: risk management, governance, budget processes, standards and guidelines, integration, business case, roles and responsibilities, leadership and knowledge of business.

3 The risk management process

3.1 Security = Risk Management[23]

Till now this paper has focused on the notion of convergence. In this section the risk management domain is explored within the context of the new security environment.To begin with risk[24] is defined, as a unified language is presently missing from the domain.This is vitally important as often different fields of study claim to be the 'owners' of risk management (eg information technology[25] and insurance) when quite oppositely, risk is enterprise-wide[26].Where there are security issues of any type, then risk management practices should be instituted.Traditionally risk was only considered to be about physical assets- 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm, to the

[21] Booz, above 5, 6.

[22] Borodzicz, above 2, 68.'The security industry is beginning to change in function and application …The simplistic conception of security- controlling physical access to the organization and controlled movement of property- may have been adequate 20 years ago. Today this would include a much larger range of risks, such as fraud, terrorism and disaster contingency plans.'

[23] Mark Merkow and Jim Breithaupt, *Information Security Principles and Practice* (2006) 27. Merkow and Breithaupt state in their principle 7 that security equals risk management. See also, Borodzicz, above 2, 50 who states:'security can be seen as risk management in practice'.

[24] Borodzicz, above 2, 52-55. Borodzicz writes that risk management can be studied using eight different approaches: historical, psychological, sociological, functionalist, management, normative, structural, and descriptive.

[25] Gurpreet Dhillon, *Information Systems Security:Text and Cases* (2007) 157.'Security risk management is not a standalone activity. It should be integrated with the systems development process. Any typical systems development is accomplished through the following steps: initiation, requirements assessment, development or acquisition, implementation, operations/maintenance, and disposal. Failure to integrate risk management with systems development results in patchy security'.

[26] Jerry A. Miccolis,'Towards a Universal Language of Risk' (1996) 43(7) *Risk Management* 46."… There should be a convergence of the treasurer's and risk manager's definition of risk… In order for senior managers to have a complete grasp of all-encompassing risk as it affects their businesses, they need to communicate the varieties of risk in a common language. Only then can they approach risk holistically, with an understanding of how the risks work independently and together, and how they could affect the bottom line when combined.'

organization.'[27] Today however the business of risk has changed.[28] Risk management[29] is now more about the organization's strategic-level initiatives[30] which encompass *both* physical and logical assets. For this reason, enterprise risk management (ERM) is about 'bringing business functions (eg finance, line management, R&D, human resources) closer together to build a common risk-based framework for better decision making…'[31]

3.2 Risk management standards and guidelines

No matter what risk analysis process is used the standard method remains the same.[32] Risk management is composed of three main parts: risk assessment, risk mitigation, and risk evaluation.[33] Will Ozier defines risk management as the process:

> 'of identifying risks, risk-mitigating measures, the budgetary effect of implementing decisions related to the acceptance, avoidance, or transfer of risk… [it also] includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-mitigating measures in a continuous or periodic cycle of … management.'[34]

While many versions of the risk management cycle are available from diverse sources- international bodies like the OECD (Organization for Economic Co-

[27] Enisa, *Glossary of Risk Management* (2008) Enisa: a European Union Agency <http://www.enisa.europa.eu/rmra/glossary.html> at 27 April 2008 4. See also, Thomas R. Peltier, *Information Security Risk Analysis* (2001) xi who states that risk is 'someone or something that creates or suggests a hazard.' Jae Shim et al, *Information Systems Management Handbook* (1999) 19. Traditionally, the common objectives of risk management included: 'avoiding, reducing or transferring risk; reducing the cost of managing risk; actively managing risk in a consistent manner throughout the organization; and providing senior management with reports on risk-management activities within the organization.'

[28] Todd L. Williams, 'An integrated approach to risk management' (1996) 43(7) *Risk Management* 22. See also, Miccolis, above 27, 48 who divides risks into two types: hazardous and non-hazardous. He categorizes risks into five different types including: physical (eg property and data), business (eg prices and reputation), legal (eg contractual and statutory), political (eg terrorism and regulation) and financial (eg securities and interest rates).

[29] Jill Slay and Andy Koronios, *Information Technology and Risk Management* (2006) 2: "a continuous process designed to assess the likelihood that an adverse event will occur, implement measures to reduce the risk that such an event will occur, and ensure that the organization can respond in such a way as to minimize the consequences of the event.' For a detailed overview of risk management see also, Wrightson and Caldwell, above 13.

[30] Institute of Risk Management, *IRM:A Risk Management Standard* (2002) AIRMIC <www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf> at 27 April 2008 2.

[31] Miccolis, above 27, 48.

[32] Thomas R. Peltier, *Information Security Risk Analysis* (2001) 5.

[33] Dhillon, above 26, 155-170.

[34] Will Ozier, 'Risk Assessment and Management' in Thomas R. Peltier (ed), *Information Security Risk Analysis* (2001) 224.

operation and Development)[35] and the ISO (International Standards Organization),[36] national standards bodies,[37] government agencies, industry-specific bodies[38] and even single organizations[39]- the cycles all encompass the same broad steps. One of the first contemporary renditions is depicted in Figure 2 (the GAO/AIMD-98-68 Information Security Management guidelines):

- Assess risk and determine needs;
- Implement appropriate policies and related controls;
- Promote awareness; and
- Monitor and evaluate policy and control effectiveness.[40]

It is worth mentioning also, that the Australian and New Zealand Standard on Risk Management AS/NZS 4360: 2004[41] is considered as leading edge[42] because it specifically addresses all forms of risk management and can be applied independent of industry type.[43] This standard, applied correctly, promotes strategic advantages.[44]

[35] Slay and Koronios, above 30, 82.The OECD Guidelines for the Security of Information Systems and Networks are subtitled 'Towards a culture of security.' One of the nine basic principles on which a culture of IS security can be founded is risk assessment.

[36] Institute of Risk Management, above 31, 5. 'Risk Assessment is defined by the ISO/IEC Guide 73 as the overall process of risk analysis and risk evaluation.' See also, ISO, *ISO/IEC Guide 73:2002: Risk management -- Vocabulary -- Guidelines for use in standards* (2008) International Standards Organization <http://www.iso.org/iso/catalogue_detail?csnumber=34998> at 27 April 2008 and Garry Roedler, *A Path to Convergence of Risk Management Standards* (July 2006) Lockheed Martin Corporation <www.incose.org/practice/techactivities/wg/risk/docs/7_Roedler_Slides_28JUN06.pdf> at 27 April 2008 3. The latter reference described ISO/IEC/IEEE 16085, as a good base for risk management principles.

[37] Slay and Koronios, above 30, 88. 'HB 231:2000 provides an exhaustive examination of the risk management process and in so doing establishes the 'strategic context', 'organizational context' and 'risk management context' within which an enterprise will carry out the risk management process.'

[38] See, eg, Dhillon, above 26, 172-178 for the I2S2 model.

[39] Peltier, above 33, 4. In many organizations risk management is synonymous with quality assurance.

[40] Peltier, above 33, 17-19. See also, Gary Stoneburner, Alice Goguen and Alexis Feringa, 'Risk Management Guide for Information Technology Systems' (National Institute of Standards and Technology, 2002) and John Walz, *Risk management in ISO standards* (2005) Sarbanes Oxley <http://www4.asq.org/blogs/sarbanes-oxley/2005/12/risk_management_in_iso_standards> at 27 April 2008.

[41] SAI Global, *Risk Management* (2008) Standards Australia <http://www.riskmanagement.com.au/> at 28 April 2008 1. See also, Slay and Koronios, above 30, 83 who state that the precursor to this standard was AS/NZS ISO/IEC 17799:2001 Code of Practice for Information Security Management.

[42] Kevin Knight, *New approach to risk management* (August 2003) SAI Global <http://www.sai-global.com/newsroom/tgs/2003-08/risk/risk.htm> at 27 April 2008.

[43] Tom Godfrey, *New risk management standard to help businesses meet ASX requirements* (14 September 2004) Standards Australia <http://www.standards.org.au/cat.asp?catid=41&contentid=197&News=1> at 27 April 2008.

[44] Godfrey, above 45.

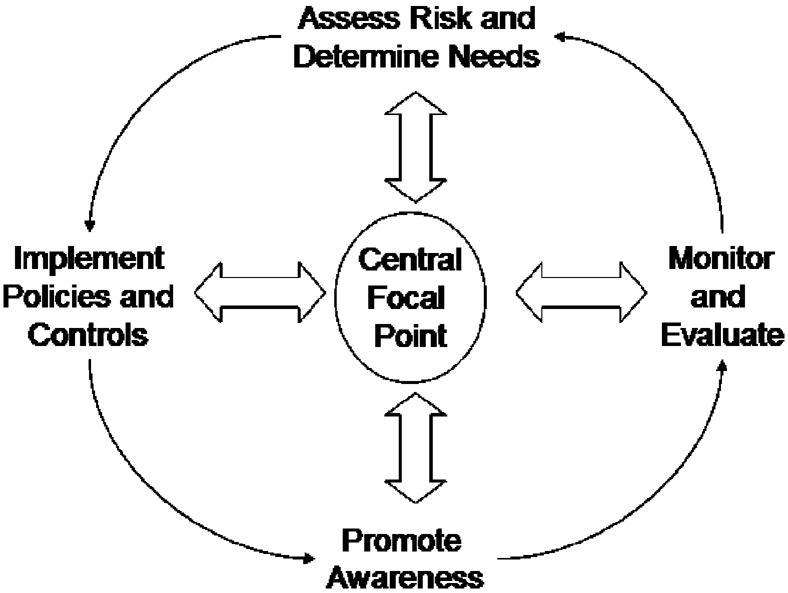

Assess Risk and Determine Needs
Implement Policies and Controls
Central Focal Point
Monitor and Evaluate
Promote Awareness

Figure 2: The steps in the risk management cycle[45]

3.2.1 Steps explained

The heart of any risk management process is a risk assessment (figure 3). Typically a risk assessment begins with identifying risks. Risks are usually categorized into different types to make assessment more meaningful. A method is then formulated to prioritize risks which typically include both quantitative and qualitative data, and may take the form of a risk score and/ or mapping exercise. A critical risk analysis is then conducted to evaluate risk-loss/risk-return values modeled against performance indicators. The risk model is then implemented and strategies are recommended to mitigate losses.[46] It is important to emphasize that risk is everybody's business. A risk assessment is considered robust if it covers a range of issues- technological, human factors, policies, third party, etc…[47]

[45] United States Government Accountability Office, above 1.

[46] Foley & Lardner LLP, *Enterprise Risk Management - Risk Intelligence and Anti-Fraud Controls* (2007) National Director's Institute at 27 April 2008 2.

[47] Dhillon, above 26, 235. Dhillon claims rightly that 'since most systems are interconnected and interdependent, any risk assessment should also consider threats that might originate elsewhere.'

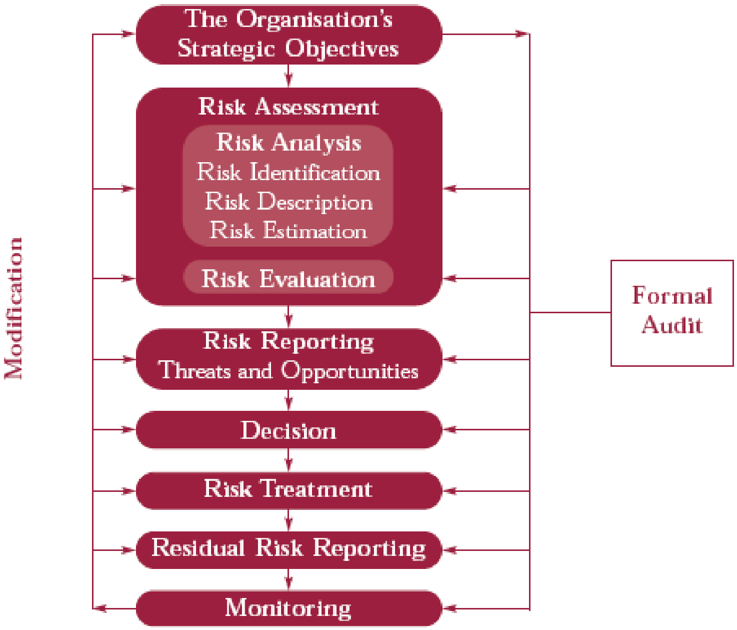


Figure 3: The risk management process[48]

3.3 What does risk management have to do with national security?

It has already been established that risk management and enterprise security go hand-in-hand. But a question that can be legitimately posed is whether or not risk management has any relevancy to national security? Figure 4 represents a contribution to knowledge as it attempts to unravel the links between terminology, processes, stakeholders, and the broader intelligence community. For the rest of the paper, these links will be explored in more detail. While it is typical to think of risk management in areas like insurance and finance, it is atypical to relate risk management to domestic terrorism. And yet, the risk management process has been embraced by the U.S. Congress and the President, post September 11, in order to strengthen against future terrorist strikes.[49] In the context of national security then, risk management can be defined as a 'strategy for helping policymakers make decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty'.[50] In the following section we investigate first the intelligence cycle, and then the likeness of the intelligence cycle to the risk management process. We pose the following hypothesis- that the intelligence cycle and risk management are converging domains and that before too long, the processes will be used interchangeably.

[48] Institute of Risk Management, above 31, 4.

[49] Wrightson and Caldwell, above 13, 8.

[50] Ibid 8. Cf chapters two and three in Jae Shim et al, *Information Systems Management Handbook* (1999) with the Wrightson and Caldwell definition- one prior to September 11 and the other after the attacks.

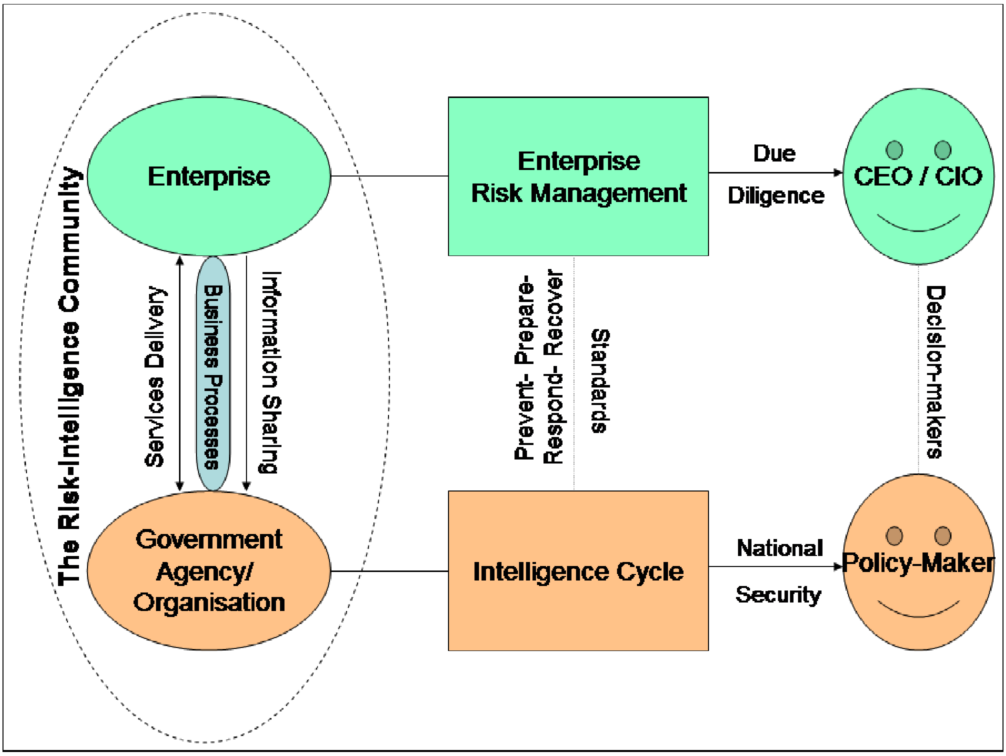


Figure 4: Making sense of the risk management and intelligence processes

4 Intelligence cycle

The common misconception is made, that the intelligence cycle is strictly something conducted by tactical military analysts. However, it is well-known that practitioners in industry widely practice intelligence-related activities for a variety of reasons, including for the purpose of competitive business intelligence (BI). Unlike the risk management process which has undergone a great deal of standardization due to compliance and other globalization factors, the intelligence cycle has remained a fairly generic framework that organizations can choose to follow completely or partially. On the national security and defense side, however, intelligence as a process is continually being improved upon, especially to combat future asymmetric attacks.

4.1 Defining the intelligence cycle

The intelligence cycle[51] can be defined as:

[51] Loch K. Johnson, 'Making the "Intelligence" Cycle Work' (1986) 1(4) *International Journal of Intelligence and Counter-Intelligence* 1 for the definitive article on describing the intelligence cycle and how it works. See also, New Zealand Qualifications Authority, *Intelligence Analysis: Demonstrate knowledge of the intelligence analysis process* (2003) New Zealand Government <www.nzqa.govt.nz/nqfdocs/units/doc/18503.doc> The NZQA define intelligence as the collective 'functions, activities, and/or organizations which are involved in the process of planning, gathering and analyzing

> 'the process by which information and data is collected, evaluated, stored, analyzed, and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, consumer.'[52]

Figures 5 shows the main phases carried out in a typical intelligence cycle; the distinct phases have remained relatively unchanged in modern times, save for the addition of the initial "requirements" phase, enabling policy makers to make a request for information (RFI).[53] This phase helps analysts to plan and better direct the intelligence effort. Data is then collected, processed, analyzed and disseminated to the appropriate stakeholders.[54] The U.S. military have developed a sophisticated "Intelligence Process Model" (IPM) that helps analysts to work through RFIs and also for decision-makers to track the status of their request(s).[55]

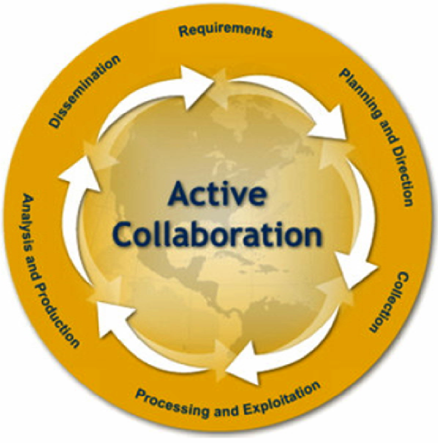


Figure 5: The intelligence cycle[56]

information of potential value to decision makers, and to the production of intelligence.' See especially, Henry H. Willis, *Using Risk Analysis to Inform Intelligence Analysis* (2007) RAND Corporation <http://www.rand.org/pubs/working_papers/2007/RAND_WR464.pdf> at 7 February 2008 3 who states that the goal of intelligence is to 'produce guidance based on available information within a time frame that allows for purposeful action.'

[52] United States Government Accountability Office, above 1, 27.

[53] Compare the intelligence cycles of: Lisa Krizan, *Intelligence Essentials for Everyone* (1999) Joint Military Intelligence College <http://www.scip.org/2_getinteless.php> at 5 February 2007 and Directorate of Intelligence, *The Intelligence Cycle* Federal Bureau of Investigations <http://www.fbi.gov/intelligence/di_cycle.htm> at 27 April 2008 1.

[54] US Intelligence Board, *Planning and Direction* (2007) <http://www.intelligence.gov/2-business_cycle1.shtml> at 10 April 2008.

[55] J.O. Miller, *Modeling the U.S. Military Intelligence Process* (2008) Department of Defense <www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf> at 27 April 2008 5.

[56] Directorate of Intelligence, *The Intelligence Cycle* Federal Bureau of Investigations <http://www.fbi.gov/intelligence/di_cycle.htm> at 27 April 2008 1.

4.2 The phases of the intelligence cycle

The *request for information* is where information needs are identified by policy makers.[57] In the *planning and direction* phase resources are identified[58] and care is taken to balance the level of intrusiveness of the request with what is legally permissible.[59] The *collection* phase follows and is where the raw information is gathered. Information comes from varied sources- it may be public, foreign or illegally intercepted[60] via satellite or other communication technology, even human intelligence (HUMINT).[61] These sources are combined with open source intelligence (OSINT) including newspapers, periodicals, foreign and domestic broadcasts (eg CNN, BBC, Aljazeera.net) and official documents (eg Commonwealth inquiries).[62] The collected data is then *processed* and made into a form that is usable by analysts. This is often where the most errors creep into the process, as different sources of data are brought together. Maintaining quality in the data sets being processed is of paramount importance. Some have referred to this processing melting pot as the 'fusion centre'.[63] It is how linkages are made between the structured and unstructured data that might be the difference between good and bad intelligence. In the *analysis*[64] *and production* phase, fused data is prepared to make intelligence products which are usually categorized by their primary use (eg indications and warning and counterintelligence).[65] Common analyses performed in these products include association, temporal and spatial charting; and link, financial, content and correlation analysis.[66] The *dissemination* phase can happen in two ways. Intelligence may be delivered to the consumer who

[57] Canadian Intelligence Security Service, *Backgrounder No. 3: CSIS and the Security Intelligence Cycle* (2004) <http://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder03.asp> at 9 March 2008 2.

[58] Miller, above 56, 3.

[59] Canadian Intelligence Security Service, above 58, 2.

[60] Ibid 3. 'In the competitive global economy of the 1990s, acquiring scientific and technological information from other countries has become increasingly important for many nations. Sometimes, this is done by covert or unlawful means.'

[61] Miller, above 56, 4. 'Organizations or agencies that operate collection assets such as satellites or surveillance equipment task those assets to gather information at specified times and places. The means and methods of collection are highly dependent on the source of the information and these sources are generally categorized into various intelligence disciplines.'

[62] Canadian Intelligence Security Service, above 58, 2.

[63] United States Government Accountability Office, above 1, 27.

[64] New Zealand Qualifications Authority, above 52, 2. 'Analysis refers to a process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions. The 'raw intelligence' collected, whether by human or technical means, is frequently fragmentary and at times contradictory. Through analysis a sorting, evaluating and interpreting of the various pieces of data occurs including an interpretation of meaning and associated significance.'

[65] Miller, above 56, 4.

[66] United States Government Accountability Office, 'Information Security Management' (U.S. Government, 1998) 27.

requested it in a 'push' action or stored to be 'pulled' at a later date.[67]

5 Integrating risk analysis into the intelligence cycle

5.1 Is risk management and the intelligence cycle linear?

Now that a brief overview of the risk management process and the intelligence cycle have been presented, let us examine the premise that both processes are not linear but network-centric, meshed, and highly collaborative. This does not mean that the actual steps or phases are contested in each process- but the manner in which stakeholders interact with one another is brought into question.[68] The move is revolutionary[69] and towards a network-centric collaboration process using a target-centric approach to interlink stakeholders and information.[70] In the new security environment convergence is acting to bring stakeholders (eg collectors, processors, analysts, policy makers) together to communicate through a centralized means to make decentralized decisions.[71] This does not mean that hierarchy is abandoned altogether in the intelligence community but that stakeholders can make use of technologies which allow for a more agile working environment. The National Infrastructure Protection Plan (NIPP)[72] in the United States presents a context for information sharing amongst the primary stakeholders. It does not mean that the new environment contains members belonging to 'one large happy family', as each organization still differs in their mission and goals.[73]

5.2 Risk management based intelligence (RMBI)

If real-time collaboration is a result of the new security environment, and private and public members of the intelligence community are sharing data (ie contributing and retrieving data), then it follows that processes too can be integrated. In a seminal paper on terrorism, Willis demonstrates how this integration is possible (figure 6). The diagram depicts the intelligence cycle on the top right, and then shows how

[67] Miller, above 56, 4.

[68] R.M. Clark, 'The Intelligence Process' in *Intelligence Analysis: A Target-centric approach* (2004) 12 15. '…The intelligence cycle has become somewhat of a theological concept: No one questions its validity. Yet when pressed many intelligence officers admit that the intelligence process *really doesn't work like that*.'

[69] Deborah G. Barger, *Toward a Revolution in Intelligence Affairs* (2005) <http://www.rand.org/pubs/technical_reports/2005/RAND_TR242.pdf> at 2 February 2008 20.

[70] Clark, above 69, 17-18.

[71] Ibid 17.

[72] Homeland Security, *National Infrastructure Protection Plan Information Sharing* (n.d.) U.S. Homeland Security at 23 April 2008 2. 'The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions.'

[73] William J. Lahneman, *The Future of Intelligence Analysis: Volume I, Final Report* (2006) Center for International and Security Studies at Maryland <http://www.cissm.umd.edu/papers/files/future_intel_analysis_final_report1.pdf> 2008 3.

information flows can be applied to enhance risk analysis. Arrows in the figure indicate how information can pass between stages of the intelligence cycle through to the risk management process and back. Willis states that risk analysis can be used to sharpen intelligence products and to prioritize resources for gathering intelligence.[74] He goes on to explain that 'risk analysis can be a tool that can help intelligence practitioners sharpen their conclusions by providing analytic support for identification of scenarios of greatest concern'.[75] It must be noted however, while risk analysis enhances intelligence, it still remains mere intelligence and far from foolproof- especially with regards to the prediction of asymmetric strikes.

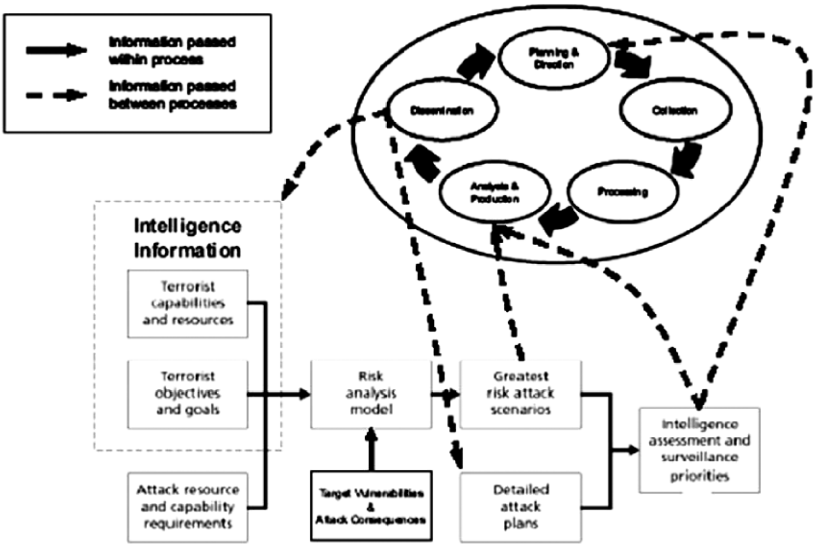

Information passed within process
Information passed between processes
Planning & Direction
Collection
Processing
Analysis & Production
Dissemination
Intelligence Information
Terrorist capabilities and resources
Terrorist objectives and goals
Attack resource and capability requirements
Risk analysis model
Target Vulnerabilities & Attack Consequences
Greatest risk attack scenarios
Detailed attack plans
Intelligence assessment and surveillance priorities

Figure 6: Connections between risk analysis and the intelligence cycle[76]

The integration of the risk management process and the intelligence cycle has been referred to as "risk management based intelligence" (RMBI). RMBI is defined as

> 'an approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source … a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and countermeasures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making

[74] Willis, above 52, 3-4.

[75] Ibid 15.

[76] Willis, above 52.

in strategic planning and for operations in tactical situations.'[77]

We can denote from the above that risk management is clearly integrated in the modern intelligence cycle; from this integration stems an even closer relationship which we can refer to here as symbiosis- ie, the trend of convergence at multiple levels including organizational,[78] process, product, and information. It is perhaps the latter convergence trend, that of information convergence, that has propelled the cultural shift in the intelligence community at large.[79] When analysts from different organizations (public or private) begin to rely on the same information sources, and are able themselves to contribute information to such causes as critical infrastructure protection (CIP), then opportunities for convergence in products, processes, and organizations emerge.[80]

5.3 Risk intelligence as a business process

If we restate Sherman Kent's classic definition of intelligence being a kind of "knowledge"[81] then we can continue to explore the notion of information convergence as enabling business processes between members of the intelligence community. In the corporate world, the recognition that 'knowledge' equated to power became prevalent in the 1990s. Organizations were quite aware that there was 'too much information, and too little knowledge'. It was at the turn of the millennium that ICT solutions also became available to solve the problem of'islands of information' through electronic resource planning systems (ERP), many of which contained a business intelligence module to go beyond data warehousing.[82] It

[77] United States Government Accountability Office, above 1, 28.

[78] Kent Anderson, 'Convergence: A holistic approach to risk management' (2007) *Network Security* 4 7.

[79] Peterson, above 9, 1. '… the world is converging around the value of information, not that information is converging around or into something else. Instead, information is the new central actor, defining the enterprise organization and its business. On one hand, information is power and a competitive weapon. In this sense, information is the chief asset of the business. Yet, on the other hand, information is also the chief risk. It is a legal and security liability and we're required to keep it exposed for what seems like forever. In the end, it is this paradox that is the catalyst for change; change which is transforming the Information-Centric Enterprise.' See also, Jill Robinson, *Risk Convergence: Future State* (2007) Ernst & Young Consulting <http://www.ey.com> at 27 April 2008 4 who describes the '… creation of a common data structure for risk and control processes and a common technology architecture supporting this effort. This common ground not only enables the Risk/Control functions to speak a single language, it also fosters communication, greater coordination, and increased understanding.'

[80] Alexandra Psica, *Destination ahead: establishing an effective risk management regime* (1 February 2007) <goliath.ecnext.com/coms2/gi_0199-6288561/Destination-ahead-establishing-an-effective.html> at 27 April 2008 2. 'Whether it's a matter of capturing information for a risk management regime, an audit, or to demonstrate regulatory compliance, the organization should aim to gather it once and use it many times. It's too costly and inefficient to ask the same question multiple times.'

[81] Andrew Rathmell, 'Towards Postmodern Intelligence' (2002) 17(3) *Intelligence and National Security* 88f.

[82] Gill, above 17, 476. 'But the construction of ever-larger databases, data warehousing and data-

should be no surprise to us then, that today "risk intelligence" (RI) has emerged as a completely new business process.[83] Two consulting companies, Deloitte[84] and Ernst and Young, have already begun to market an RI framework. Figure 7 represents an authentic convergence of the risk management process and the intelligence cycle. Risk intelligence enterprises are those organizations that are characterized by their future vision, ability to bridge silos and speak a common language, conduct impact assessments, weigh up the vulnerabilities, allocate resources appropriately, act with a risk conscious spirit, and even pursue risk for the purposes of higher rewards.[85] The risk intelligent chief information officer (CIO)[86] is someone who practices risk intelligence. And just like any other framework or process, there are differing levels of sophistication that can be attained.[87]

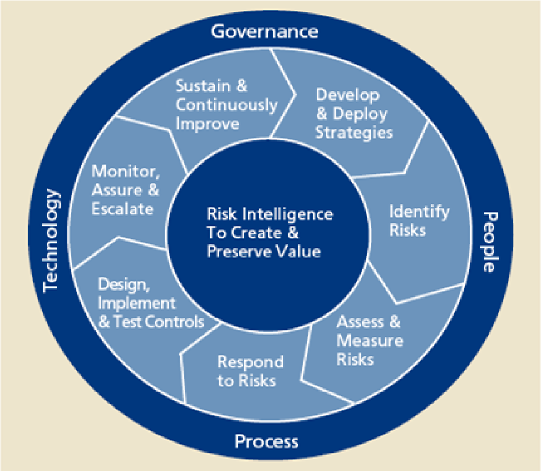

Governance
People
Process
Technology
Sustain & Continuously Improve
Develop & Deploy Strategies
Identify Risks
Assess & Measure Risks
Respond to Risks
Design, Implement & Test Controls
Monitor, Assure & Escalate
Risk Intelligence To Create & Preserve Value

Figure 7: The risk intelligence framework[88]

5.4 Problems associated with the risk intelligence process

A number of problems plague the intelligence community in the new security

mining, though of great significance in intelligence, cannot 'solve' intelligence problems without a process of targeting, careful evaluation of information and human analytical skills.'

[83] B. Azvine et al, 'Operational risk management with real-time business intelligence' (2007) 25(1) *BT Technology Journal* 155. Risk intelligence should not be confused with real-time business intelligence (RTBI), despite the fact that the terms are closely allied. RTBI attempts to deliver 3 critical components: 'real-time information delivery, real-time business performance analysis, real-time action on the business processes.'

[84] Robinson, above 80, 4. 'Many organizations are now looking at convergence models to integrate risk and control processes and create a common framework for assessing and monitoring the organization's risks.'

[85] Layton, above 10, 2.

[86] Lee Dittmar and Bill Kobel, 'The Risk Intelligent CIO' (2008) 55(3) *Risk Management* 42.

[87] Nathan Houser and Sean Conlin, *Creating Risk Intelligence: A High Level "How To" Guide for Program Managers* (2006) Deloitte <management.energy.gov/06W_RMconHou.ppt> at 27 April 2008 6.

[88] Layton, above 10, 5.

environment. It does not mean that risk intelligence will not work, but governments need to understand that these challenges are not trivial, and attempt to combat them with longer-term initiatives. Even if we take the naïve view that implementing convergence is 'easy', we still require competent analysts who understand the data and can deal with the increasing complexity of technical products.[89] For many, the answer lies in professionalizing the security-risk industry. Training programs for analysts by a single accreditation organization is widely recommended. Providing intelligence in a timely manner is another issue, alongside the capability to simplify the information being gathered so it is meaningful and can be applied into action by decision makers.[90] In addition, what kind of data will reside in the intelligence system for the conduct of all-source analysis by organizations should not be forgotten as a key challenge- after all garbage in/garbage out (GIGO).[91] Perhaps the biggest challenge at hand however, is governance- how do you bring the intelligence community together within an integrated culture,[92] break down the barrier of secrecy, and still maintain limits to information accessibility based on RFIs. Trust in people and systems, along with enforceable policies and procedures will be paramount in this emerging environment.

6 Conclusion

The overarching benefit of convergence in maintaining national security is strategic, ie keeping one step ahead of the enemy to prevent terrorist attacks in order to minimize the element of surprise. Convergence has the ability to make a reduction in overhead and duplication and to streamline once separate security groups and organizations.[93] Today convergence is about remaining successful;[94] and more than that it is about giving life to new opportunities and emergent benefits that cannot be achieved individually.[95] At the moment the trend towards a unified security program[96] seems to be about reducing risks and increasing control through

[89] Lahneman, above 74, 3. 'The report concluded that, if current practices continue, the intelligence community (IC) of 2020 will experience an imbalance between the demand for effective overall intelligence analysis and the outputs of the individually-oriented elements and outlooks of its various analytic communities.'

[90] Azvine, above 83, 155.

[91] Ibid 160. 'Good data often leads to visionary and profitable decision making. Poor data quality is often the cause of bad strategic decisions and inaccurate financial and management reporting.'

[92] Lahneman, above 89, 10. 'The U.S. intelligence community is the "Community that Isn't." It is a series of nearly autonomous organizations, each with its own way of doing business. The analytic portion of the IC reflects the fragmentation of the overall intelligence enterprise. Such a fragmented approach is at odds with the need for greater knowledge sharing to enable effective analysis of dispersed threats and other issues.'

[93] Anderson, above 79, 6.

[94] David Silverstein, *It's All About Convergence* (2007) Inc.com <http://www.inc.com/resources/office/articles/20070601/silverstein.html> at 27 April 2008.

[95] Anderson, above 80, 6.

[96] Ibid.

quality intelligence. However, one could also be critical of the security industry at large and point out, that the trend towards a 'super' converged system is destined to failure because monolithic systems are subject to singularities, and could create more complications than answers. Some may even say the effort towards convergence is a waste of money, time and energy because anti-terrorism capabilities are a fallacy.[97] Is the technology[98] available today propelling us all toward a future environment that may create even more problems for us as a society? Time will tell.

[97] Gill, above 17, 478. 'Given what is known about the modus operandi of those carrying out the attacks, it is extremely unlikely that such a piece of information exists. Nor was it just a case of the system failing 'to join the dots' between pieces of data so that warning could have been provided though this starts to get closer to the real failure of US intelligence: the failure of processing and analysis.'

[98] Pathak, above 8, 569. 'This shift is being driven by the "convergence" of IT security methods with those of the more traditional physical security methods.'

7

Could terrorists acquire and detonate nuclear weapons? A scenario

Nick O'Brien

Associate Professor, Graduate School of Policing, Faculty of Arts, Charles Sturt University

Abstract

The aim of this paper is to examine whether a terrorist group such as Al Qaeda (AQ) has the intent and capability to detonate a crude nuclear device in a western city with New York as the chosen city for the scenario. The methodology used is historical examination of select terrorist attacks, a review of available information to determine whether it would be possible for terrorists to obtain the necessary components and expertise to construct a weapon and subsequently transport the device across international boundaries. Some of the likely social and legal implications of such an attack are also considered using the aftermath of the July 2005 attacks in London as an example. The main findings indicate that, at a minimum, senior AQ personnel have discussed obtaining a nuclear weapon and that it may be possible to obtain the materials and expertise needed to construct such a weapon and transport it across international boundaries. Any anti-terrorism legislation introduced following such an attack will need to be proportionate to the actual threat to avoid alienating communities.

Keywords: terrorism, nuclear weapons, weapons of mass destruction, CBRN, social impacts, mass murder, legislation

1 Introduction

For Al Qaeda (AQ) to successfully detonate a nuclear device, four elements would need to be present. A desire to kill as many as possible; acquisition of plutonium or highly enriched uranium (HEU); people with the requisite skill set willing to assist AQ and transportation of the weapon or its components to the target city. It is also likely, but not necessary, that a suicide operative would be used. This paper will examine information available to determine whether terrorists have a desire to commit mass-murder and whether they could obtain, transport and detonate a nuclear device. Political reaction following the London attacks of July 2005, including suggested legislative changes, will be explored to ascertain whether comments in the scenario about curtailment of some human rights could be far-fetched. Possible dangers to human rights will be highlighted.

It used to be said that terrorists wanted a lot of people watching and listening and not a lot dead (Jenkins, 1975, p.15). At the time the comment was made it was true. Ethno-nationalist terrorists had their objectives which were often around ousting colonial powers and whilst there were some indiscriminate killings often the violence was aimed at police or troops. The kidnapping and subsequent murder of eleven Israeli athletes at the Munich Olympics in 1972 had the dual objectives of the release of prisoners and the acquisition of world-wide publicity for the Palestinian cause. The motives for aircraft hijackings in the years that followed never involved the mass murders of those on board. Whilst there were a few notable exceptions, such as the bombing of Pan Am flight 103 over Lockerbie, Scotland, Jenkins's comments in 1975 remained true. Then came Al-Qaeda and the desire for mass murder by a non-State actor.

2 A desire to inflict mass casualties?

Al Qaeda (AQ) was founded in 1988 by Usama bin Laden (UBL) and Abdullah Azzam, following the announcement from Moscow that the Soviets were pulling their troops out of Afghanistan (9/11 Commission Report, ND, p. 56). An example of the desire to kill as many as possible was the first World Trade Center attack in 1993. On February 26th 1993, Ramzi Yousef, a Sunni extremist, and others planted a bomb at the World Trade Centre in New York, and whilst six people died Yousef stated that he had planned to kill 250,000 people (9/11 Commission Report, ND, p. 72). Whilst it is not known whether bin Laden knew of the attack, he apparently often lauded the attackers as 'role models'.

In 1998 came the start of AQ's pursuit of the US and 'the west'. On 7th August 1998 AQ were responsible for the bombings at the US Embassies in Dar es Salaam, Tanzania and Nairobi, Kenya, which killed over 300 people and wounded more than 5000 (Hoffman, 2006, p.87).

Then came the big one. On 11th September 2001, AQ carried out what has become known as the '9/11' attacks in the United States. As a result of this attack some 2996 people lost their lives (www.september11victims.com). In October 2004, a video tape of UBL was made available to al-Jazeera. In this tape, UBL admits that AQ were behind the 9/11 attacks with the following words, "…al-Qaeda spent $500,000 on the September 11 attacks, while America lost more than $500 billion, at the lowest estimate, in the event and its aftermath. That makes a million American dollars for every al-Qaeda dollar, by the grace of God Almighty" (ed. Lawrence, 2005, p.242).

It didn't stop there. On 22nd December 2001 British citizen, Richard Reid, attempted to detonate a 'shoe bomb' on American Airlines flight 63 from Charles de Gaulle International airport, Paris to Miami International airport, Florida (Gunaratna, 2002, p.13). Reid admitted to being a member of AQ and to having been trained in an AQ camp, although some experts have questioned his membership of AQ as he confessed to interrogators almost immediately (Stern, 2003, p.277).

Briton Sajid Badat should have detonated a bomb on another plane at the same time as Reid, but withdrew from the attack (O'Neill & McGrory, 2006, p.229). Forensic tests indicated that 'the detonator cords for Reid and Badat's devices were two parts of the same length of material' (O'Neill & McGrory, 2006, p.231).

On 28th November 2002, two attacks happened in Mombasa, Kenya. In the first attack a suicide bomber detonated in the Paradise Hotel killing a total of 14 people (Corbin, 2003, p.346). In the second attack two surface to air missiles, also known as Man Portable Air Defence Systems (MANPADS), were fired at an Arkia Airways Boeing 757 as it took off from Mombasa Airport. The plane contained 260 Israeli tourists who were returning to Israel. The attack was unsuccessful. Corbin (2003, p.347) indicates that AQ was behind the attack.

On May 16th 2003 five suicide bombs detonated in Casablanca, Morocco, killing some 45 people. The terrorists have been described as 'AQ Self Starters' (Benjamin & Simon, 2005, p.27).

On 15th November 2003, terrorists carried out a suicide attack against two synagogues in Istanbul killing 25. This was followed by suicide attacks against the British Consulate General and the Hong Kong and Shanghai Banking Corporation (HSBC) in Istanbul killing 26. Turkish police arrested a number of people trained and directed by Al Qaeda (Chandler & Gunaratna, 2007, p.50).

On 27th February 2004, SuperFerry 14 was bombed in the Philippines, killing more than one hundred people. It is likely that the Abu Sayaaf Group (ASG) was behind the attack and ASG claims to be connected to AQ (Elegant, 2004).

On March 11th 2004, 191 people were killed when terrorists detonated ten bombs on trains in Madrid, Spain. Whilst the attacks were AQ in style, and were carried out by Muslim men, the links to AQ are unclear. Benjamin and Simon describe the attacks as, 'not the handiwork of Usama bin Laden. Instead it was an homage – both honour and emulation – to him and his ideas' (2005, p.6).

On 7th July 2005 bombs exploded on three trains and one bus in London, England, killing 56 people including four suicide attackers. In a video broadcast on 19th September, Ayman Al Zawahiri, deputy leader of AQ stated, "London's blessed raid is one of the raids which Jama'at Qa'idat al-Jihad (Al Qaidah of the Jihad Group) was honoured to launch… In the Wills of the hero brothers, the knights of monotheism – may God have mercy on them, make paradise their final abode and accept their good deeds…." (Report of the Official Account of the Bombings in London on 7th July 2005, p.21). It is known that two of the London bombers, Mohammed Sidique Khan and Shezad Tanweer, visited Pakistan between November 2004 and February 2005 and it is assessed as likely that they had some contact with AQ figures (Report into the London Terrorist Attacks on 7 July 2005, p.12).

On 9th November 2005, suicide bombers detonated in three hotels in Amman, Jordan killing 56 people including the three suicide bombers. Al Qaeda in Iraq, also known as the 'al-Qaeda organisation in the Land of the Two Rivers' claimed the attack (BBC, 2005).

On 10th August 2006, twenty-one people were arrested for allegedly plotting to put bombs on 10 aircraft travelling from the UK to the US. A Scotland Yard spokesperson said that, "mass murder on an unimaginable scale" had been disrupted (BBC, 2006). A senior US official told CNN that the intelligence that uncovered the plot, "makes very strong links to Al Qaeda" (CNN, 2006). This alleged plot is particularly disturbing as had it been successful, death on the scale of 9/11 could have occurred. Also it is an example of AQ attempting to attack one of the most hardened industries in recent times. The conclusion can be drawn that AQ will attempt to attack the airline industry in the future.

On June 29th and June 30th 2007 an attempt was made to detonate car bombs in both London and Glasgow (BBC, 2007). Had either of the attacks been successful, the death toll could have been considerable.

The above does not attempt to give a comprehensive list of recent serious terrorist attacks and terrorism in Iraq and Afghanistan have been deliberately omitted as it could be argued that those countries are facing insurgency rather than conventional terrorism. The examples are given to indicate that the threat from terrorism is both real and serious. Indeed, the *EU Terrorism Situation and Trend Report* (2008, p.11) states that, "a total of 1044 individuals were arrested for terrorism-related offences in 2007. This is an increase of 48 percent compared with 2006". Comments made by Jonathan Evans, the Head of the UK domestic intelligence service, MI5, also indicate that the threat is substantial. In a speech to the *Society of Editors* in 2007, Mr Evans stated that MI5 had identified 2000 individuals who, "posed a direct threat to national security and public safety, because of their support for terrorism." He went on to say "we suspect that there are as many again that we don't yet know of" (Evans, 2007).

3 Al Qaeda's desire to obtain nuclear devices

But has AQ an interest in acquiring a nuclear device? Kluger (2001) states that it was well known in the intelligence world that Bin Laden was seeking nuclear weapons as far back as the mid nineties. In 1998 UBL was interviewed by Al-

Jazeera. During the interview the subject of nuclear weapons was raised and UBL congratulated the Pakistanis for having possession of a nuclear weapon, "because we consider it the Muslim's right to have it…". The Al-Jazeera reporter asked UBL, "Can this be taken as confirmation that you are seeking to acquire this weapon?" UBL replied, "…There is a duty on Muslims to acquire them, and America knows today that Muslims are in possession of such a weapon, by the grace of God Almighty" (ed Lawrence, 2005, p.72).

In 2002 it was reported that AQ spokesman, Suleiman Abu Gheith, stated on a website that the "Islamic Nation" had the right to kill 4 million Americans, including 2 million children. The following words were used, "We have not reached parity with them. We have the right to kill 4 million Americans - 2 million of them children - and to exile twice as many and wound and cripple hundreds of thousands. Furthermore, it is our right to fight them with chemical and biological weapons, so as to afflict them with the fatal maladies that have afflicted the Muslims because of the [Americans'] chemical and biological weapons" (Middle East Media Research Institute, 2002). Whilst nuclear weapons were not mentioned, the desire to commit mass murder is evident.

To make matters worse, in 2003, Sheikh Nasir Bin Hamd Al-Fahd published a treatise entitled, 'The Legal Status of Using Weapons of Mass Destruction Against Infidels.' Al-Fahd stated, "If a bomb that killed ten million of them and burned as much of their land as they have burned Muslims' land were dropped on them, it would be permissible, with no need to mention any other argument. We might need other arguments if we wanted to annihilate more than this number of them" (Uphoff, 2004). Al-Fahd subsequently retracted the treatise but it is currently available on the internet. Michael Scheuer, a former head of the CIA's Bin Laden Unit and author of a number of books on terrorism takes little regard of the retraction believing instead that Arab regimes use such recantations to, "deceive Western governments and publics." He says, "[f]ew Muslims, radical or otherwise, put stock in such reversals because their prevailing and probably accurate assumption is that the individual's reversal of view was prompted by threats or physical punishment directed at him or his family" (Scheuer, 2008, p.74).

In 2004, *The Atlantic Monthly* published comments by Scheuer. He stated,

> "Mid-to-Late 1996: CIA's Bin Laden unit acquired detailed information about the careful, professional manner in which al-Qaeda was seeking to acquire nuclear weapons ... there could be no doubt after this date that al-Qaeda was in deadly earnest in seeking nuclear weapons. The report was initially suppressed within CIA, and then published in a drastically shortened form. Three officers of the Agency's Bin Laden cadre protested this decision in writing, and forced an internal review. It was only after this review that this report was provided in full to Community leaders, analysts, and policymakers" (The Atlantic.com, 2004).

On the subject of AQ's desire and willingness to acquire and use a nuclear weapon, Scheuer concludes,"…it is impossible to argue that bin Laden is not pursuing such a weapon or that al-Qaeda would not use it if acquired" (Scheuer, 2008, p.74). Micah Zenko reviewed de-classified intelligence estimates on nuclear terrorism and believes that the evidence revealed a number of findings one of which was that "terrorist groups are obsessed with obtaining a nuclear weapon" (2004, p.88).

4 How a nuclear device could be obtained

The case that Al Qaeda's desires to obtain and would use nuclear weapons has been made. But would it be possible for a terrorist group to get hold of such a device?

To carry out a nuclear attack terrorists would either have to construct a device, be given one by a rogue state or steal a device. To construct a device, terrorists would need to obtain either Highly Enriched Uranium (HEU) or plutonium (Barnaby, 2003, p.111). Whilst it would not be easy to construct a weapon there are many publications both in print and electronic which provide general specifications on how to construct a device. But here at least there is some disagreement. Matthew Bunn from Harvard University's Belfer Center gave evidence before the Committee on Homeland Security and Governmental Affairs in the United States Senate in April 2008. Bunn's opinion was that a sophisticated terrorist group could construct a crude nuclear device if they had HEU or 'separated plutonium' (Bunn, 2008). Al Venter an author and military correspondence discusses the "urban legend" that a "good university with an advanced scientific facility could, with solid application, build the bomb". Venter describes the idea as "nonsense" (Venter, 2007, p.7).

Frank Barnaby, who trained as a nuclear physicist and who has worked at the UK's Atomic Weapons Research Establishment and who now works for the Oxford Research Group, specialising in nuclear issues and the terrorist use of weapons of mass destruction (WMDs), disagrees with Venter. Barnaby believes that a "group of two or three people with appropriate skills could design and fabricate a crude nuclear explosive. He continues,

> "It is a sobering fact that the fabrication of a primitive nuclear explosive using plutonium or suitable uranium would require no greater skill than that required for the production and use of the nerve agent produced by the AUM group and released in the Tokyo underground" (Barnaby, 2004, p.36).

Barnaby's comments raise two important issues mentioned at the beginning of this paper. Could a terrorist group attract people with "appropriate skills' and could they get hold of either plutonium or highly enriched uranium?

Khan and Moore (2001) reported that two Pakistani nuclear scientists, Sultan Bashiruddin Mahmood and Abdul Majid, held lengthy discussions in 2001 with UBL and his deputy, Ayman Zawahiri, about nuclear, chemical and biological weapons. The scientists were, at the time, in custody in Pakistan. The talks were described as "academic" but the two said that UBL was "intensely interested" in the weapons.

Pakistani officials described the scientists as, "very motivated" and "extremist in their ideas."

Whilst the above indicates that AQ can attract extremists with some expertise, the case of A.Q. Khan, a man reportedly described by former CIA director, George Tenet, as "at least as dangerous as Osama Bin Laden" (Corera, 2006, p.xiii), is perhaps more disturbing.

Abdul Qadeer Khan, through a formidable network, was responsible for providing Pakistan with nuclear weapons. But not only did he provide the technology to Pakistan, he also built a global network centred around secret procurement of nuclear technology. Corera asserts that Khan eventually "began looking for customers and shifting his exceptional business model from import to export" (ibid). Frantz and Collins (2007, p.XIV) describe Khan's organisation as a "nuclear Wal-Mart" opening that he

> "had done more to destabalize the world's delicate nuclear balance than anyone in history, emerging as the common thread woven through today's most dangerous nuclear threats… the sheer scale of what Khan wrought is breathtaking, and so is the apparent ease with which he sold his wares."

In the days before the collapse of the Soviet Union the nuclear standoff, although potentially apocalyptic, was clear, 'you bomb us and we'll bomb you'. The world had the power to destroy itself many times over, but there was symmetry – a balance between two opposing powers. AQ has started to change that balance. On September 11th 2001 the USA raised the nuclear alert status from defcon 6 to defcon 2 which is the level below making the launch code operable. It is likely that Russia did the same so thousands of nuclear devices were ready to go with a three minute lead time (Caldicott, 2002, p.IX). Whilst many do not agree with nuclear weapons, the fact is we have them. The cold war situation whilst potentially devastating was controllable with only a few countries having membership of one of the most exclusive clubs in the world. Then along came A. Q. Khan. He did not just change the symmetry, he shattered it forever. If terrorists ever manage to detonate a nuclear device it is likely that Khan's work will materialise in the intelligence and evidential trail.

It is possible that a terrorist group could gather together people with the expertise to construct a crude nuclear device. But could they get hold of the HEU or plutonium necessary to construct a nuclear device? Bunn (2008) believes that answer is 'yes' commenting that both nuclear weapons and their "essential ingredients exist in hundreds of buildings in dozens of countries, with security measures that range from excellent to appalling – in some cases, no more than a night watchman and a chain-link fence." To support his case he describes an attack in 2007 on the Pelindaba nuclear facility in South Africa on the night of November 8th 2007 where hundreds of kilograms of weapon-grade HEU are stored. Apparently four armed men were able to disable perimeter detection devices, enter the control room and shoot a worker. The intruders stayed on the facility for 45 minutes. The South

African government has not released details of the investigation so it is not possible to state the intentions of the attackers. However, Bunn believes that the risk of nuclear theft is greatest in the former Soviet Union, Pakistan and at HEU fuelled research reactors worldwide (ibid).

There are other worrying cases. For example, in January 2007 the *New York Times* (Sheets & Broad, 2007) reported that a Russian man, Oleg Khinsagov, attempted to sell 100 grams of uranium in Tbilisi which had been refined to make it nuclear weapons grade. The amount was a sample and Khinsagov claimed he had access to two to three kilograms. Fortunately the 'buyer' was a Georgian agent so Khinsagov was arrested and sentenced to eight and a half years in prison. Further information revealed that the uranium had been enriched to "nearly 90 percent U-235, according to Russian and American government analyses obtained by *The New York Times*." Apparently as little as 25 kilograms of uranium enriched to 90% is needed to construct a nuclear bomb (Sokova et al 2007).

Then there is the issue of the supply of both expertise and nuclear material by so called 'rogue states'. According to a report prepared for the US Congress in February 2008, five countries are nuclear states according to the Nuclear Non-Proliferation Treaty (NPT): China, France, Russia, the UK and the USA. "Four other states – India, Israel, Pakistan and North Korea – have nuclear weapons. The first three have not signed the NPT. North Korea announced its withdrawal from the NPT January 10, 2003" (Kerr, 2008). One estimate is that North Korea has enough fissile material to produce between ten and fifteen nuclear weapons (Gallucci, 2006, p.53).

Iran is also suspected of pursuing a nuclear weapons programme. A November 2007 *National Intelligence Estimate* stated that it was likely that Tehran stopped its nuclear weapons programme in Autumn 2003 but that it was "keeping open the option to develop nuclear weapons" (National Intelligence Council, 2007). However in June 2008, the Foreign Ministers of France, Germany, the UK, the USA, China, Russia and the EU wrote to their opposite number in Iran offering to work with Iran on a nuclear energy programme. The letter contained some comments which gives cause for concern,

> "But in recent years, Iran's relationship with the international community has been overshadowed by growing tension and mistrust, since there remains a lack of confidence in Iran's nuclear programme. We have supported the IAEA's (*International Atomic Energy Agency*) efforts to address this with Iran but successive IAEA reports have concluded that it is not able to supply credible assurances about the absence of undeclared nuclear materials and activities in Iran" (Rice et al, 2008).

The Israelis are very concerned about a nuclear Iran and on 4th June 2008, Israeli Prime Minister Ehud Olmert warned that drastic measures were needed to stop Iran obtaining nuclear weapons and that it must be indicated to Iran that there would be severe consequences if it did obtain the bomb. Earlier in June the Israeli Deputy Prime Minister, Shaul Mofaz, stated that it was likely that military strikes against

Iran to stop them getting nuclear weapons looked "unavoidable" (BBC, 2008). To back his point the *New York Times* reported that in June 2008, more than 100 Israeli military planes had taken part in manoeuvres which appeared to be a rehearsal for an attack on Iran's nuclear facilities (Gordon, 2008). Whilst Israel's response could be political posturing or muscle flexing, there should be no doubt of its concern over a nuclear Iran, partly because it fears an attack but also because it fears that Iran could supply expertise and/or material to a terrorist group.

5 Transporting a nuclear device or its components

If terrorists could get access to the expertise to build a nuclear device and the uranium or plutonium necessary to cause a nuclear explosion, could they smuggle either a bomb or the component parts into the USA? The US has land boundaries of over 12,000 kms and a coastline of nearly 20,000 kms (CIA, 2008). Each year, billions of dollars worth of drugs are smuggled into the country and thousands of illegal immigrants enter the country. Matthew Bunn in his testimony to the Committee on Homeland Security and Governmental Affairs in the United States Senate in April 2008 stated that he believed that a terrorist group could deliver a bomb to Washington, New York and "other major cities around the world" (Bunn, 2008).

In 2002 the American *ABC News* tested US defences against smuggling of nuclear material into the country.

> "On July 4, in a train station in Europe, a suitcase containing 15 pounds of depleted uranium, shielded by a steel pipe with a lead lining, began a secret 25-day, seven-country journey. Its destination was the United States….ABCNEWS' project was designed with the help of three of the world's leading authorities on nuclear terrorism: Dr. Thomas Cochran, senior scientist and nuclear weapons expert with the Natural Resources Defense Council, an environmental group that lent the depleted uranium to ABCNEWS for the investigation; Dr. Fritz Steinhausler of Stanford University in California and the University of Salzburg in Austria; and Allison of Harvard's Belfer Center. "It is a perfect mockup," said Cochran. "It replicates everything but the capability to explode.""

On 29th July 2002 the suitcase arrived at the Port of New York. The uranium was undetected in any of the countries it transited and was not detected in the USA (Ross et al 2002).

Clearly the US is now considering ways a terrorist group could smuggle nuclear material into the country. US Homeland Security Secretary, Michael Chertoff, believes that the possibility of terrorists smuggling a nuclear device into the US on a private plane is a "very real threat". Consequently authorities have launched a $4 million study to ascertain whether radiation detection equipment can pick up signs of radioactive materials on board passenger planes (Hall, 2008).

6 Scenario-based possible consequences

At the beginning of this paper it was stated that four elements need to be present for the unthinkable to happen:

- A desire to kill as many as possible;
- acquisition of plutonium or highly enriched uranium (HEU);
- people with the requisite skill set willing to assist AQ
- and transportation of the weapon or its components to the target city.

It could be argued that all the elements are in place.The unthinkable could happen, although it would be extremely challenging to achieve.

Bunn (2008) describes the threat of nuclear terrorism as "among the most urgent threats to America's security."The question must be asked,'Is nuclear terrorism today just a possible plot line in a novel or Hollywood film or is the spectre of nuclear terrorism a reality?' As terrorists have never detonated a nuclear device a short scenario follows to illustrate what could happen.Vincent-Lancrin (2006) states,"[f] utures scenarios do not aim to predict the future nor picture what a desirable future could be like,but merely to provide stakeholders with tools for thinking strategically about the uncertain future before them". Scenarios are also academically sound as they "bear considerable similarity to the more traditional Harvard case study Model" (Victor, 1999, p. 100). Because there is no "right answer" scenarios can therefore "stimulate thought" (ibid). They allow the reader to make judgements about the future (Litchfield & Fan, 2007, p.56) and inevitably all will not come to the same conclusion.

> *It has happened. What terrorism watchers fear most, a nuclear device has exploded in New York. At least half a million people have been killed by the initial explosion and many more will die later.The nuclear alert status in the US has been raised to defcon 2 and nuclear powers worldwide take similar action. Planes with nuclear weapons on board take off and nuclear submarines are alerted to be ready to strike.The US President and Vice President have been moved to a nuclear bunker. Stock Markets around the world have plummeted. Food stores around the world struggle to keep up with demand as people stockpile tins of food from Sydney to Southampton and Moscow to Mombasa. There are long queues outside petrol stations as people fear that fuel will become scarce.*
>
> *Following the initial panic the situation calms.There is worldwide condemnation of the attack and services are held in religious institutions from churches to synagogues, mosques and Buddhist temples.There are however media reports of some people dancing in the street with joy in some Middle Eastern countries. World leaders line up to support the US, promise assistance to the injured and stand firmly behind the US President who vows to find the perpetrators of this hideous act.*
>
> *Presidents and Prime Ministers in 'the West' approach Security Services and police asking them what powers they need to prevent such an attack in their*

> *country. More money is promised to counter-terrorism units, the military and to counter-proliferation efforts. Each leader quietly hopes that there will not be a link to their own country in the investigation. Draconian powers to arrest and detain suspects without charge and intrude into the private lives of citizens are proposed and accepted. All Imams now have to be licensed to preach and their permits renewed every two years. New powers are granted to exclude people from countries on the say so of an elected government minister. Glorification of terrorism becomes an offence, although it is not clear what 'glorification' means. Police get powers to stop and search without reasonable cause. The political opposition stays silent as the mood of the country and the media supports the powers. Senior politicians condemn multiculturalism saying it is outdated and there are sporadic incidents of attacks on Muslims and mosques. The use of monitored CCTV cameras grows exponentially in towns and cities across the world.*
>
> *Senior Muslim leaders speak out against the powers commenting that they are plainly aimed at the Muslim community and they will alienate the youth. Stop and search statistics start to reveal that young men of Asian/Pakistani appearance are twenty times as likely to be stopped by police as white youths.*
>
> *After three months a film is released to Al-Jazeera, it is Usama Bin Laden claiming responsibility for the attack and threatening another unless all western governments leave Saudi Arabia and the Middle East, he says that the next attack could occur in any country – at his will. He calls on the world to convert to Islam.*
>
> *The President of the United States calls for a meeting to consider a nuclear strike on the Pakistan Afghan border as intelligence sources believe that this is the most likely location of UBL. The President also publicly states that the US will attack Iran if it pursues its nuclear ambitions. How the attack will happen is left open.*

The above is just a microcosm of what could happen – the reality could be much worse. There might never be a return to the normality of the days of a pre nuclear attack by terrorists.

7 Comparisons with the July 2005 London Attacks

Set against the fatalities that would occur if a nuclear bomb was detonated in New York, the attacks in London of July 2005, although tragic, could be described as a relatively minor affair. But do the possible reactions in the scenario described above compare in any way with what happened after the London attacks?

On 3rd August 2005, Conservative Party politician David Davis, who was standing for the leadership of the Party published an article in the UK's *Daily Telegraph* newspaper (Davis, 2005). In the article he described multiculturalism as outdated and stated that the Human Rights Act should be reviewed and if necessary, repealed.

In the same month the Home Office published plans to deport people from the UK. Included were proposals to: amend human rights laws to prevent legal obstacles to deportation, create a list of foreign preachers to be excluded from the UK, and to make justifying or glorifying terrorism anywhere an offence (BBC, 2005). In September 2005 the Home Secretary published plans to extend the time suspected terrorists could be held without charge from two weeks to three months (ibid).The latter proposal was subsequently defeated in the House of Commons but the matter is still extant in the UK with proposals to be able to hold suspected terrorists for forty-two days without charge.

On 19th August 2005, *epolitix.com* published an interview with former Conservative Party Chairman Lord Tebbit. In the interview Lord Tebbit stated that, "the Muslim religion is so unreformed since it was created that nowhere in the Muslim world has there been any real advance in science, or art or literature, or technology in the last 500 years". During the interview Lord Tebbitt also said that he opposed "the concept of a multicultural society" (epolitix, 2005).

Whilst it is difficult to judge whether the comments and proposals in the aftermath of the London attacks contributed to radicalisation, a poll of Muslims and the general population by *Populus* a year after the attack showed some disturbing results. Seventy-nine percent of those Muslims surveyed said that they had experienced more abuse and hostility since the bombings with 74% believing that they were viewed with suspicion by their fellow citizens (Populus, 2006).

The case of the London attacks suggests that curtailment of civil liberties and human rights is a probability rather than a possibility should terrorists detonate a nuclear device.

8 Dangers to human rights

Paul Wilkinson, Professor of International Relations at the University of St Andrews cautions against both overreaction and under-reaction in response to mass casualty attacks, he comments that "general repression… could destroy democracy far more rapidly and effectively than any campaign by a terrorist group" (Wilkinson, 2006, p.61). He also comments that there is "abundant" evidence to show that an overreaction actually serves the cause of the terrorist (p.82).

This view is supported by Geoffrey Robertson QC who comments that the lessons of history have illustrated that it is important not to overreact and that abandoning basic human rights is a form of surrender which serves to give terrorists what they desire (Robertson, 2006, p.553).

Waleed Aly, when discussing the use of torture by US authorities, makes the valid point that revolutionary movements thrive on this type of treatment (Aly, 2007, p.206). Draconian legislation will have the same effect on the Muslim population: alienation. This cannot be good and will not assist moderate Muslims to prevent radicalisation in their communities.

The threat of terrorists' use of weapons of mass destruction is the greatest man-made threat to our civil rights but it is also the greatest threat to our freedom (Bobbitt, 2008, p.245). If the bomb does explode and the mushroom cloud is seen over a major western city major loss of life will occur and the radiation fall-out will affect people for decades. Politicians will be forced to act and introduce new legislation which will impact on our freedoms. Governments have a responsibility to protect their citizens. It is inevitable that such protection will impact on both privacy and liberty. We expect, however, such legislation to be open and the action of police to be accountable in the courts. As Australian lawyer Julian Burnside points out, "[i]n a climate of fear, protection of human rights becomes extraordinarily difficult" (2007, p.159). If the bomb goes off there will be climate of fear, understandably so. It will be important to ensure that any subsequent legislation does not serve to alienate sections of the community and assist radicalisation.

9 Conclusion

It is evident that AQ has discussed obtaining nuclear weapons. Only a few people know whether this was terrorist bluster, an interest designed to divert western resources towards prevention, or the first step down a path that could see a nuclear device detonated in a western city. There would appear to be a clear danger both from so called 'rogue states,' and from individuals, who would sell either technology, expertise or the HEU or plutonium needed to construct a device.

Some experts on nuclear weapons technology believe that it is possible that terrorists could obtain and detonate a nuclear device. Indeed one academic from Harvard University gave evidence before the Committee on Homeland Security and Governmental Affairs in the United States Senate in April 2008 stating that he believed that terrorists could deliver a nuclear bomb to New York.

Following the 9/11 attacks in the United States many countries introduced stronger anti-terrorism legislation, including the US, Australia and the UK. The reactions from politicians in the UK following the attacks in July 2005 indicates the probability of the introduction of legislation that will impinge on civil liberties should a nuclear device be detonated by terrorists. Unless this legislation is in proportion to the actual threat it may succeed in alienating and radicalising the communities who could do most to assist in preventing terrorism.

Any government has an unenviable task in deciding what counter-terrorism legislation to introduce in the case of a massive loss of life. It will be important to ensure that legislation is not born of a knee-jerk reaction to a tragic situation. It should be thoughtful and considered with a 'sunset clause' to ensure that it is reviewed after a two year period. The most important bodies to ensure that the legislation is appropriate and does not go too far will be the media, the opposition and ultimately the electorate. There may be people who will regard the introduction of new legislation as being too liberal and others may claim that the laws are too severe. If that happens, perhaps the government will have got it about right.

References

(n.d.). Retrieved from http://www.september11victims.com/september11victims/victims_list.htm

9/11 Commission Report. New York: W.W. Norton.

Allison, G. (2004). *Nuclear Terrorism.* London: Constable & Robinson Ltd.

At-a-glance: New Terror Plans. (2005, September 16). Retrieved July 5, 2008, from BBC News: http://news.bbc.co.uk/2/hi/uk_news/politics/4179128.stm

Barnaby, F. (2004). *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction.* London: Granta Publications.

BBC. (2005, November 10). *"Al-Qaeda' claims Jordan attacks.* Retrieved June 18, 2008, from BBC News: http://news.bbc.co.uk/2/hi/middle_east/4423714.stm

BBC. (2006, August 10). *'Airlines terror plot' disrupted.* Retrieved June 18, 2008, from BBC News: http://news.bbc.co.uk/2/hi/uk_news/4778575.stm

BBC. (30, June 2007). *Blazing car crashes into airport.* Retrieved June 18, 2008, from BBC News: http://news.bbc.co.uk/2/hi/uk_news/scotland/6257194.stm

BBC. (2008, June 20). *Israelis 'rehearse Iran attack'.* Retrieved June 24, 2008, from BBC News: http://news.bbc.co.uk/2/hi/middle_east/7465170.stm

Benjamin, D. &. (2005). *The Next Attack.* London: Hodder & Stoughton.

Bobbitt, P. (2008). *Terror and Consent.* Camberwell: Penguin Group.

Bunn, M. (2008, April 2). *The Risks of Nuclear Terrorism and the Next Steps to Reduce the Danger.* Retrieved June 22, 2008, from Belfer Center: http://belfercenter.ksg.harvard.edu/files/bunn-nuclear-terror-risk-test-08.pdf

Burnside, J. (2007). *Watching Brief.* Carlton North: Scribe Publications.

Caldicott, H. (2002). *The New Nuclear Danger.* Carlton North: Scribe Publications.

Chandler, M. &. (2007). *Countering Terrorism.* London: Reaktion Books.

CIA. (2008, June 19). *The World Factbook - United States.* Retrieved June 23, 2008, from CIA: https://www.cia.gov/library/publications/the-world-factbook/geos/us.html

CNN. (2006, August 10). *Police: Plot to blow up aircraft foiled.* Retrieved June 18, 2008, from CNN.com: http://www.cnn.com/2006/WORLD/europe/08/10/uk.terror/index.html

Corbin, J. (2003). *The Base.* London: Simon & Schuster.

Corera, G. (2006). *Shopping for Bombs.* Carlton North: Scribe Publications.

Davis, D. (2005, August 3). *Why Cultural Tolerance Cuts Both Ways.* Retrieved July 5, 2008, from Telegraph: http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2005/08/03/do0302.xml

Elegant, S. (2004, August 23). Retrieved June 18, 2008, from Time: http://www.time.com/time/magazine/article/0,9171,501040830-686107,00.html

epolitix.com. (2005, August 19). *Tebbit: Cricket Test Could have Stopped Bombings.* Retrieved July 5, 2008, from epolitix.com: http://www.epolitix.com/latestnews/article-detail/newsarticle/tebbit-cricket-test-could-have-stopped-bombings/

Europol. (2008). *EU Terrorism Situation and Trend Report* . The Hague: Europol.

Evans, J. (2007, November 5). *Intelligence, counter-terrorism and trust.* Retrieved June 19, 2008, from MI5 Security Service: http://www.mi5.gov.uk/output/Page562.html

Gallucci, R. (2006). Averting Nuclear Catastrophe: Contemplating Extreme Responses to U.S.Vulnerability. *The Annals of the American Academy of Political and Social Science*, 53.

Gordon, R. &. (2008, June 20). *U.S. Says Israeli Exercise Seemed Directed at Iran*. Retrieved June 24, 2008, from New York Times: http://www.nytimes.com/2008/06/20/washington/20iran.html?_r=1&scp=1&sq=israelis+rehearse+iran+attack&st=nyt&oref=slogin

Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror.* Carlton North: Scribe Publications.

Hall, M. (2008, June 18). *Nuke Detectors Being Tested on Private Jets.* Retrieved June 23, 2008, from USA Today: http://www.usatoday.com/news/washington/2008-06-18-nukes_N.htm?POE=click-refer

Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.

House of Commons. (2006, May 11). Retrieved June 18, 2008, from Official-Documents.gov.uk: http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf

Intelligence & Security Committee. (2006). *Report into the London Terrorist Attacks on 7 July 2005.* Norwich: The Stationary Office.

Jenkins, B. (1975). International Terrorism: A New Mode of Conflict. *International Terrorism and World Security*, 15.

Kerr, P. (2008). *Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends.* Congressional Research Service.

Khan, K. &. (2001, 12 December). *2 Nuclear Experts Briefed Bin Laden, Pakistanis say*. Retrieved June 20, 2008, from Washington Post: http://www.hvk.org/articles/1201/89.html

Kluger, J. (2001, November 12). *Osama's Nuclear Quest.* Retrieved June 19, 2008, from Time: http://www.time.com/time/magazine/article/0,9171,182894-1,00.html

Lawrence, B. (. (2005). *Messages to the World – The Statements of Osama Bin Laden.* London: Verso.

Litchfield, & R. Fan, J. (2007). Sequential & Simultaneous Multiple Explanation: Implications for Alternative Consideration When Response Options are not Provided. *Judgment and Decision Making*, 54-69.

Middle East Media Research Institute. (2002, June 12). *Why we fight America.* Retrieved June 20, 2008, from Middle East Media Research Institute: http://www.memri.org/bin/articles.cgi?ID=SP38802

National Intelligence Council. (2007, November). *Iran: Nuclear Intentions and Capablities*. Retrieved June 24, 2008, from National Intelligence Estimate: http://www.dni.gov/press_releases/20071203_release.pdf

O'Neill, S. &. (2006). *The Suicide Factory.* London: Harper Collins.

Populus. (2006, July). *Muslim 7/7 Poll*. Retrieved July 5, 2008, from Populus: http://www.populus.co.uk/the-times-itv-news-muslim-77-poll-050706.html

Rice, C. (2008, June 12). *Text of Latest Diplomatic Offer to Iran*. Retrieved June 24, 2008, from Institute for Science and Internatioanl Security: http://www.isis-online.org/publications/iran/Diplomatic_Offer_16June2008.pdf

Robertson, G. (2006). *Crimes Against Humanity.* Camberwell: Penguin Group.

Ross, B. S. (2002, September 11). *Customs Fails to Detect Depleted Uranium.* Retrieved June 23, 2008, from abc News: http://abcnews.go.com/WNT/story?id=129321&page=1

Scheuer, M. (2008). *Marching Towards Hell.* New York: Free Press.

Sheets, L. &. (2007, January 25). *Smuggler's Plot Highlights Fears Over Uranium.* Retrieved June 23, 2008, from New York Times: http://www.nytimes.com/2007/01/25/world/europe/25nuke.html?_r=1&n=Top/Reference/Times%20Topics/People/B/Broad,%20William%20J.&oref=slogin

Sokova, E. P. (2007, January 26). *Recent Weapons Grade Uranium Smuggling Case: Nuclear Materials are Still on the Loose.* Retrieved June 23, 2008, from CNS: http://cns.miis.edu/pubs/week/070126.htm

Stern, J. (2003). *Terror in the Name of God.* New York: Harper Collins.

The Atlantic Monthly. (2004, December). *How Not to Catch a Terrorist.* Retrieved June 20, 2008, from Atlantic.com: http://www.theatlantic.com/doc/200412/anonymous

Uphoff, K. (2006, December 10). *Osama Bin Laden's Mandate for Nuclear Terror.* Retrieved June 20, 2008, from The Jewish Institute for National Security Affairs: http://www.jinsa.org/articles/index.html/function/view/categoryid/1701/documentid/2762/history/3,2360,655,1701,2762

Venter, A. (2007). *Allah's Bomb: The Islamic Quest for Nuclear Weapons.* Guildford: Lyons Press.

Victor, D. (1999, December). Using Scenarios and Vignettes in Cross Cultural Business Communication Instruction. *Business Communication Quarterly*.

Vincent-Lancrin, S. (2006). What is Changing in Academic Research? Trends and Future Scenarios. *European Journal of Education*, Vol 41, No 2.

Wilkinson, P. (2006). *Terrorism versus Democracy.* Abingdon: Routledge.

Zenko, M. (2006). Intelligence Estimates of Nuclear Terrorism. *The Annals of the American Academy of Political and Social Science*, 87-102.

8

Questioning national security powers

David Vaile

Executive Director, Cyberspace Law and Policy Centre, University of New South Wales

Abstract

The worlds of political spin-doctoring and “intelligence” should be kept clearly separate; hundreds of thousands of ex-Iraqis can explain why. There are nasty local precedents emerging where this separation has broken down, and breathlessly over-stated claims that open-ended surveillance is essential or even effective for improving overall ‘security’ of the population have been uncritically allowed to undermine the balance between oppressive and increasingly unaccountable ‘law enforcement/national security’ powers, and the rights and expectations of citizens to the rule of law which had been hard-won over centuries of contested legal evolution.

Keywords: politics, intelligence, surveillance, security, national security, law enforcement, power, citizen rights, law

9

With reckless abandon: Haneef and Ul-Haque in Australia's 'War on Terror'

Mark Rix

Senior Lecturer, Graduate School of Business, University of Wollongong

Abstract

This paper considers the political and social implications of the manner in which Australia has prosecuted the so-called 'war on terror'. It does this by investigating relevant aspects of Australia's anti-terrorism legislation and the performance of Australian security and law enforcement agencies, namely, the Australian Security and Intelligence Organisation (ASIO) and the Australian Federal Police (AFP). Focusing on the Haneef and Ul-Haque cases, the paper will consider how the political climate created by the former Federal Government's legislative approach to the war on terror has influenced the performance of these organisations. By focusing on these two cases, the paper will demonstrate how racial, ethnic and religious stereotyping have informed and shaped Australia's conduct of the war on terror. It will investigate the real potential for social division, and heightened national *insecurity*, that flows from the use and propagation of these stereotypes. The paper will also highlight the unfairness and prejudice that are inherent to racial and religious stereotyping. Finally, the paper will consider whether the Rudd Labor Government's approach thus far to the war on terror differs in any significant measure from that of its predecessor and evaluate the prospects for real, progressive change.

Keywords: 'war on terror', anti-terrorism legislation, ASIO, AFP, national security, human rights, due process

1 Introduction

Australia's anti-terrorism legislation contains onerous provisions and powers which are supposedly necessary to protect the country from the threat of terrorism and from terrorist attacks. These have been subjected to rigorous scrutiny, critique and debate that have focused in the main on the legislation's implications for human rights and civil liberties, the rule of law and integrity of the legal system, and executive government and parliamentary democracy in this country. The question of whether the legislation has strengthened or weakened Australian national security has also been a reasonably strong theme. While the legislation's impacts on social and religious harmony have not been completely out of sight of most commentators, its racial and religious undercurrents and their social effects have generally been peripheral or secondary concerns. This paper is centrally concerned with investigating these undercurrents and exploring their implications for Australians of Islamic faith and their ability to live as citizens, residents or visitors in this country free from discrimination, harassment and persecution.

In taking up this central concern, the paper will focus on two recent terrorism cases, the Haneef and Ul-Haque affairs. Both of these are instructive, for they reveal the racial and religious preconceptions that lay just beneath the surface of Australia's anti-terrorism enactments and the political climate in which the legislation was enacted and which in turn it has helped to perpetuate. As will be demonstrated in the investigation of these two cases, the political climate has also enabled the security and law enforcement agencies to exceed their warrant and mandate and to violate the human rights and legal entitlements of terror suspects and to do so largely with impunity. Racial and religious stereotyping, implicitly associating people of Islamic faith and of Middle Eastern, South Asian or other 'dubious' origin with the threat of terrorism, has been a key underlying factor in the creation and attempted perpetuation of this political climate.

2 Haneef, Ul-Haque and the 'War on Terror': the Howard Government's political and social legacy

The manner in which the Haneef and Ul-Haque cases have been handled by the Rudd Labor Government since it came to office in November 2007 is important for it gives some insight into new Government's thinking about the terrorist threat and how best to counter it legislatively and in other ways. The Government appears to be aware that these cases, particularly Haneef's, have triggered a degree of scepticism and unease in the Australian community about the way in which the war on terror had been prosecuted by the former government and the law enforcement and security agencies. Central to these concerns are the former Government's attempts to use the legal system as a vehicle for pursuing its political and ideological agenda in the run-up to the 2007 Federal election and the manner in which this was seen to compromise or undermine long-established legal principles and presumptive rights.

There was in all this also a measure of disapproval of the way in which the Howard Government sought to manipulate public opinion by fomenting racially motivated anti-Islamic fear and hatred in the wider community. In going to the lengths it did in attempting to make a negative example of Haneef (and, to a lesser extent, Ul-Haque) the Government only ended up handing its critics and detractors with evidence that the anti-terrorism legislation was riddled with flaws and excesses inimical to individual rights and liberties. For, as became clear as the cases unfolded and publicly unravelled, if people like Haneef and Ul-Haque could be treated in the way they have been then so potentially could any member of the Australian community regardless of their ethnicity or religious predisposition. Just as the law is supposed to be blind to race, religion and the like so ironically, and paradoxically, could the anti-terrorism legislation be used to incriminate individuals of any or all races and religions. However, in the war on terror it just happens to be individuals of Islamic faith and of Middle Eastern or South/Central Asian origin who are, so to speak, in the firing line.

In a 2006 paper analysing Australia's anti-terrorism legislation, the present author pointed out with particular reference to the Anti-Terrorism Act (No. 2) 2005:

> Just as with the [Act's] preventative detention and control provisions, the crime of sedition can be used by the authorities to persecute and harass members of the communities they regard as presenting a threat to Australia's national security. This could have the effect of splitting up the Australian community into those regarded as posing no actual or potential threat and those who are suspected of posing such a threat. In a general climate of suspicion, fear and anxiety, this will almost certainly run the distinct risk of converting resentment and hostility into violent and terroristic intent. This is a sort of self-fulfilling prophecy providing the Government with a ready-made defence against charges that it is unfairly targeting certain groups and individuals. In any event, a more deeply and dangerously divided Australian community could well be the result (Rix 2006: 437).

The paper also noted the fact that, now as then almost a truism, it is Muslim communities and individuals, and people of Middle Eastern origin, who are most at risk from the persecution, harassment and arbitrary detention permitted in this and other anti-terrorism acts under the pretext of preventing terrorism and protecting national security (see, e.g., Lynch 2007 and Aly 2007 which explore a number of these issues; all but one of the 19 terrorist organisations listed on the Australian Government's national security website are self-proclaimed Islam organisations the only exception being the Kurdistan Workers Party (PKK) (see Australian Government n.d.)).

The Security Legislation Review Committee (SLRC, also known as the Sheller Committee) voiced similar concerns in its June 2006 Report noting the 'profound impact' which recent (unspecified) events had had on Muslim and Arab communities.

It identified increasing fear, alienation and distrust of authority as the 'biggest impacts' on these communities.[1] To address this issue, and to allay the fears and concerns of Muslim and Arab communities, the SLRC recommended that all Australian governments embark on a community education program to explain the meaning and intent of the anti-terrorism legislation (SLRC 2006: 8; for a more comprehensive analysis and discussion of the SLRC Report, see Rix 2008). This campaign should also address prejudices and fears in the wider (non-Muslim) community.

The Parliamentary Committee on Intelligence and Security (PJCIS) released its Review of Security and Counter Terrorism Legislation in December 2006. Chapter 3 of the Review was devoted to assessing the impact of the 'new security environment', particularly the anti-terrorism legislation, on Arab and Muslim Australians. It pointed to the rise in 'prejudicial feelings' towards these Australians in the wake of the terrorist bombings in the United States, Britain, Spain and other parts of Europe, and Indonesia and noted that similar feelings had been awakened in other western countries. As the Review noted, the effects on these communities and their members of the rise in such feelings include fear and insecurity, discrimination and the perception that anti-terrorism laws are selectively applied to Muslim Australians, and confusion and uncertainty created by the sweeping offences and loose definitions of terrorism, terrorist organisation and terrorism-related offences contained in the legislation. All this has led to alienation and withdrawal by many Muslim Australians (including children) from the wider community, exacerbated by some of the sensationalist media coverage of police investigations into alleged terrorist organisations and suspects.[2] To counter these effects, the Review recommended that the Federal Attorney-General's Department improve its efforts to make comprehensive information about the anti-terrorism legislation available in appropriate community languages and generally to ensure that the Australian public has access to this information. To reinforce this, the Review suggested that information about appeal, redress and complaint mechanisms relating to the security and law enforcement agencies and the media be widely disseminated. The PJCIS Review also recommended that Australia's strategy to counter terrorism include 'a commitment to the rights of Muslims to live free from harassment and enjoy the same rights extended to all religious groups in Australia (PJCIS 2006: 38).' With respect to the media, and in order to promote social cohesion, a statement on the

[1] The 'profound impact' which the unspecified events and the anti-terrorism legislation had had on Muslim and Arab communities is discussed at some length in the submissions to the SLRC from organisations such as the Human Rights and Equal Opportunity Commission, the Public Interest Advocacy Centre, the Australian Muslim Civil Rights Advocacy Network and the Federation of Community Legal Centres (Vic).

[2] The PJCIS review took submissions on the effect of the anti-terrorism legislation on Arab and Muslim communities from organisations including the Islamic Information and Support Centre of Australia in association with Ahlus Sunnah Wal Jama'ah Association (confidential), Australian Muslim Civil Rights Advocacy Network, the Human Rights and Equal Opportunity Commission and the Public Interest Advocacy Centre.

importance of informed and balanced reporting should also be a part of Australia's counter terrorism strategy.

Some of these themes were taken up by Robert McLelland, the new Attorney-General, in a speech to the Security in Government Conference held in Canberra in December 2007 (this conference has been held annually since 2004). According to McLelland, the then recent change in Government presented an opportunity to introduce a new approach to national security, including the adoption of a broader perspective on the terrorist threat. This new approach would, like the old, include 'hard intelligence and law enforcement'. But, in addition, 'steps to promote greater inclusiveness and opportunity' would be important elements (McLelland 2007). In calling for greater inclusiveness and opportunity, McLelland observed that 'a terrorist threat in Australia has as much prospect of emanating from a disgruntled and alienated Australian youth as it does from the awakening of a sleeper cell planted by an overseas terrorist organisation.' Fighting terror thus not only required 'determination', it also required just as surely an approach which promoted 'justice, the rule of law, genuine peace and inclusive development (McLelland 2007).'

A measure of commitment to justice and the rule of law is demonstrated in the new Government's decision to hold an inquiry into the Haneef Case. During 2007, this case became a cause célèbre subjecting the former Government and its anti-terrorism legislation to intense media and public scrutiny in the lead up to the Federal election. The then Opposition had even called for a full judicial inquiry into the affair. It is worth recounting the particulars of the case.

3 The case of Dr Mohamed Haneef

On Monday, 2 July 2007 Dr Mohamed Haneef, an Indian doctor who worked as a registrar at the Gold Coast hospital in Queensland, was arrested and later charged (14 July) with recklessly supplying support to a terrorist organisation. This and other terrorist organisation offences were introduced into the Commonwealth Criminal Code by the Securiy Legislation Amendment (Terrorism) Act 2002. Before being charged, Haneef had been arrested and subsequently questioned and detained under provisions of the Crimes Act 1914 as amended by the Anti-Terrorism Act 2004 (for analysis of these offences and provisions as they apply in the Haneef case, see LCA 2008 and Lynch, McGarrity and Williams 2008; see also Rix 2006).

In 2006, Haneef had given a SIM card to his cousin Sabeel Ahmed who lived in England. Sabeel Ahmed was subsequently charged with withholding information about a terrorist attack after his brother, Kafeel Ahmed, was found behind the wheel of the jeep that was crashed into the Glasgow airport building on 30 June 2007. The day before attempted car bombings outside two London nightclubs, in which Kafeel also was a central figure, had been thwarted. A little over two weeks after Haneef was charged, the Commonwealth Director of Public Prosecutions dropped the charge on the basis that there was insufficient evidence to support a conviction (ABC 2007). Writing in the *Sydney Morning Herald* on 14 April 2008, David Marr reports that the Australian Federal Policy and the Commonwealth Director of Public Prosecutions both seem to have ignored evidence that Mohamed Haneef was innocent. The British police had become aware of this evidence soon after they began investigating Kafeel's activities in 2007. Marr writes, 'The case against Dr Haneef always centred on allegations that his second cousin Sabeel Ahmed, a doctor practising in England, was part of a terrorist organisation. But in the Old Bailey on Friday [11 April] Mr Justice Calvert-Smith accepted there was "no sign" of Ahmed "being an extremist or party to extremist views".' (Marr 2008) This means that neither Sabeel Ahmed nor the SIM card could have been involved in Kafeel's failed car bombings in London and Glasgow.

Before being charged, Dr Haneef had been detained in custody for 12 days and was held for a further two weeks after being charged. Hours after Dr Haneef had been granted bail on the terrorism charge by a magistrate (16 July), the then Immigration Minister Kevin Andrews cancelled Dr Haneef's immigration (work) visa. This he did on the grounds that Haneef failed the Migration Act's character test, in line with secret evidence Andrews claims was supplied to him by the Australian Federal Police, and placed him in immigration detention. He was released to home detention on 27 July and allowed to return to India on 29 July (his visa remained cancelled). In August, Justice Spender of the Federal Court reinstated Dr Haneef's visa, a decision upheld by the Full Bench of the Federal Court in December quashing an appeal by Andrews (Peatling 2008).

In a press interview announcing that the judicial inquiry into the Haneef affair would be conducted by former NSW Supreme Court Judge the Honourable John Clark QC, Attorney-General Robert McLelland explained:

> It is essential that we maintain public confidence in Australia's counter-terrorism measures. Australians are entitled to be reassured that their national security agencies are functioning as effectively as they can be, and that our counter-terrorism laws are being appropriately enforced. Understandably, the Haneef case has prompted some in the community to question this (McLelland 2008).

The inquiry will examine and report on matters relating to the case including the arrest, detention, charging, prosecution and release of Dr Haneef and the cancellation of his visa. Among its other terms of reference, the inquiry will consider the operational performance and effectiveness of Commonwealth agencies involved in the matter, the effectiveness of cooperation and coordination between Commonwealth agencies and the relevant state law enforcement agencies and, finally, identify any deficiencies in the relevant anti-terrorism legislation and the relevant operational and administrative procedures and arrangements of Commonwealth agencies.[3]

[3] It is not clear whether the inquiry will consider why the Australian Federal Police investigation into Dr Haneef remained active well into 2008. As at the week beginning 31 March 2008, 9 AFP officers were still working on the case with the total cost of the investigation approaching

While the Attorney-General made clear that Mr Clarke would conduct the inquiry in a manner which did not compromise the safety and integrity of national security information or endanger ongoing investigations and overseas trials either impending or underway (as in the UK), there would nevertheless be 'opportunities for public input into the inquiry, including by advertising for submissions and conducting public forums on the operation of counter-terrorism laws and arrangements (McLelland 2008).' All relevant Commonwealth agencies, including the Department of Immigration, had pledged their full cooperation with the inquiry which would at its conclusion release a report that would be made public (to be supplemented by a confidential report if circumstances dictated).

Asked about the concerns he had expressed with 'the broader suite of counter-terrorism laws that operate at the moment' and the provisions they contain such as control orders and preventative detention, the Attorney-General had an interesting and suggestive answer. Picking up on the interviewer's reference to the Sheller Committee (SLRC) recommendations, McLelland pointed out that the Government is giving consideration to those recommendations, as well as to the review into the questioning and detention powers contained in the ASIO Act conducted by the Parliamentary Joint Committee on ASIO, ASIS and DSD in 2005 and to the Australian Law Reform Commission's recommendations on the sedition provisions of ATA (No. 2) (for an analysis of the reports and recommendations produced by these various bodies, see Rix 2008). 'One of the specific terms of reference of Mr Clarke is to report on the effectiveness of counter-terrorism laws in respect to the facts surrounding the Haneef matter and', commented the Attorney-General, 'obviously, there may be some relevant matters that we will have to consider in light of those recommendations (McLelland 2008).'

The inquiry into the Haneef case opened on 30 April. This happened to be the very day on which *The Australian* newspaper reported in a front-page story that the former Immigration Minister Kevin Andrews would testify to the inquiry that the Australian Federal Police had withheld from him the important information cited above proving that Sabeel Ahmed was not a member of a terrorist organisation and was not involved in the attempted London nightclub and Glasgow airport bombings (McKenna 2008). This issue not only raises important questions about Mr Andrews' veracity and trustworthiness, but also about the AFP's role in the Haneef debacle. The specific concerns relating to the AFP, besides the allegation of withholding evidence, include whether it ignored the crucial evidence proving that Haneef was innocent of the charges brought against him and, a related point, whether the British police had actually provided the AFP with the information demonstrating that Sabeel Ahmed was not involved in the London and Glasgow

AUD 8 million (Maley and O'Brien 2008). In a letter published in *The Australian* on 4 April, one correspondent wrote that it reminded him of the man 'who was fixated on horses. He was digging deep into a load of horse manure dumped at a local tip, chuckling away to himself and muttering, "There has to be a horse in here somewhere."'

bombings. But Mr McLelland has refused to expand the Clarke inquiry's terms of reference to enable it to investigate the relationship between the AFP and its British counterparts, specifically, whether the British police had supplied the AFP with the information that exonerated Sabeel Ahmed and, indirectly, Mohamed Haneef as well. This is just one of the shortcomings of the Clarke inquiry that have attracted considerable media attention and public disquiet.

Lawyers also have concerns that the powers granted the inquiry are not adequate, specifically, that it does not have the power to compel witnesses to give evidence or to face cross-examination and cannot compel the production of documents as would a Royal Commission or a properly constituted commission of inquiry (ABC 2008; McKenna 2008). Mr Clarke rejected a direct request from Stephen Keim SC, representing Dr Haneef, that the inquiry to be provided with the power to compel witnesses to give evidence. Stephen Keim made his request on the opening day of the inquiry, which could be its only public hearing (Maley 2008 and 2008a). This is a another concern, for Mr Clarke has indicated that interviews with witnesses would be conducted in private, ensuring that much of the evidence presented before the inquiry would not be made public. While he has undertaken to post transcripts of interviews on the inquiry website, this will be only done after the removal of any information which is regarded as being prejudicial to national security (Maley 2008a).

Denying the Clarke inquiry the powers of a Royal Commission or commission of inquiry gives rise to a further concern, that witnesses would not have indemnity against either defamation or self-incrimination meaning that they could potentially face civil law suits. Thus, many witnesses could either decide not to appear before the inquiry or, even if they did, refuse to answer questions (Maley 2008a).

In a press conference on the opening day of the inquiry (30 April), the Attorney-General emphasised how important it was that Mr Clarke be able to conduct the inquiry in a manner which gave due regard to the importance of protecting 'sensitive national security information' and to ensuring that 'ongoing investigations' (including presumably into Dr Haneef) and criminal trials such as those currently under way in the United Kingdom would not be prejudiced (McLelland 2008a). Mr Clarke's rejection of the request to seek expanded powers for the inquiry and his undertaking to 'sterilise' interview transcripts suggest that he is not about to throw down the gauntlet to his political masters, at least as far as compelling witnesses to provide evidence and making available unexpurgated records of interview are concerned. A preoccupation with the sanctity of national security information and current investigations and criminal trials had been a feature of the press conference which Mr McLelland hosted in March where he announced the terms of reference of the Clarke inquiry. In light of this and the other concerns with the Clarke inquiry, the Attorney-General's assurance that 'should at any stage he [Mr Clarke] come to the government and indicate that the absence of cooperation of any witness, any agency, or any person, is impeding a full and proper inquiry…then we will certainly have regard to any request, should it be made to provide powers of compellability in terms of documents and witnesses' seems more than a little hollow (McLelland 2008a).

4 The case of Izhar Ul-Haque

The Ul-Haque case is much less celebrated but in its own way even more disturbing than the Haneef affair. For while this case brought to light serious flaws, deficiencies and excesses in the anti-terrorism and related legislation, the Ul-Haque case exposed the climate of fear, suspicion and contempt for the rule of law created by the former Government's legislative approach to the war on terror. In this climate the AFP and ASIO were emboldened to exceed their authority and mandate by flagrantly violating the human rights of terror suspects, in this instance, Izhar Ul-Haque and committing criminal offences in the attempt to secure a conviction. It does bear at least one important similarity to the Haneef case, however, in that it also demonstrates the racial, ethnic and religious stereotyping, explicit or implicit, which helped to define the former Australian Government's approach to the war of terror enshrined as this is in its legislative response. As with Haneef, the details of the Ul-Haque case need to be briefly recounted. Before doing so, however, a number of preliminary points about this case need to be made.

Because the Ul-Haque case did not become a cause célèbre during the election campaign it did not expose the former Government, and its legislative response to the terrorist threat, to nearly the same level of media and public scrutiny as the Haneef affair generated. And, because the Ul-Haque case put more of the focus on the activities of the law enforcement and security agencies the Government was largely shielded from direct scrutiny and criticism. For this reason, it is able to be dealt with in a more condensed manner than the Haneef case. Nevertheless, as will be seen below, NSW Supreme Court Justice Michael Adams' findings regarding the behaviour of the AFP and ASIO in the Ul-Haque case demonstrate that it is at least as significant in that it exposes the dangers of the lack of a strict accountability regime for these agencies. This is a point that will be taken up below.

Izhar Ul-Haque was charged with training with the Pakistan-based terrorist group Lashkar-e-Toiba (or, Lashkar-e-Tayyiba as it is otherwise known) in 2003 well before it had been classified as a terrorist organisation by the United Nations. The Criminal Code Amendment (Hizbollah) Act 2003 and similar legislation proscribing Hamas and Lashkar-e-Toiba passed later the same year either pre-empted or ignored the Al-Qaida and Taliban Sanctions Committee of the UN Security Council which, for example, only added Lashkar-e-Toiba to the Consolidated List of individuals and groups belonging to or associated with Al-Qaida on 2 May 2005 (UN n.d.; neither Hamas nor Hizbollah is included on the Al-Qaida groups Consolidated List last updated on 17 October 2007 and neither is on the Taliban groups Consolidated List which, in any event, currently has no entities listed).

On November 5th 2007 in the NSW Supreme Court, Justice Michael Adams found that all records of interview with Ul-Haque tendered by the Australian Federal Police as evidence were inadmissible forcing the Director of Public Prosecutions to withdraw the case just before a jury was empanelled (R v Ul-Haque [2007] NSWSC 1251). The AFP had also tried to elicit information from Ul-Haque about the terror suspect Faheem Lodhi by questioning him in a maximum security gaol for more than two hours but without first cautioning him or informing his lawyer of the interrogation (O'Brien 2008). Two AFP officers had demanded that Ul-Haque turn informant against Lodhi (by wearing a wire and spying for them) who was subsequently convicted and gaoled for 20 years for conspiring to bomb the national electricity grid.[4] When he refused to do so, Ul-Haque was threatened that there would be serious and adverse consequences for him. While Ul-Haque had briefly trained with Lashkar-e-Toiba in early 2003, the law enforcement authorities had admitted to him that they accepted that his connection to the organisation had nothing to do with Australia but instead was because of his opposition to the Indian presence in Kashmir. The AFP records of interview were found to be inadmissible because of the improper and oppressive conduct of the AFP (and ASIO) officers involved, and because of the inextricable links between AFP and ASIO including the disclosure by the AFP to ASIO of what Haneef had said in interview. Justice Adams also found that two ASIO officers had committed the criminal offences of kidnapping and false imprisonment at common law and another offence under the Crimes Act (R v Ul-Haque [2007] NSWSC 1251). He also found that the conduct of the ASIO officers amounted to a gross breach of the powers they had been granted under a search warrant which had been issued to them.

In response to the collapse of the Ul-Haque case, the AFP initiated an inquiry headed by former NSW Chief Justice Sir Laurence Street in which former NSW Police Commissioner Ken Moroney and former head of the Defence Signals Directorate Martin Brady were also included (the Federal Attorney-General's Department and the Inspector-General of Intelligence and Security, Ian Carnell, were other additions to the inquiry). The inquiry was charged with investigating the circumstances of the case and recommending changes to law enforcement agency policy and practice such as new procedures and protocols for improved communication and cooperation between the AFP and ASIO in joint operations (O'Brien 2008).

At the conclusion of its review of the conduct of Ul-Haque case, the Street inquiry produced 10 recommendations on how in future joint agency counter-terrorism investigations could be better managed. One of its findings, for example, was that closer and more effective cooperation between the AFP and ASIO had been hampered by 'mistrust, poor communication and a lack of basic equipment, such as "secure" desktop phones' (Maley and O'Brien 2008)[5]. There was also an absence

[4] The NSW Court of Criminal Appeal quashed Lodhi's appeal against his conviction, a ruling recently upheld by the High Court of Australia.

[5] This is a curious finding in light of the inextricable links between the two organisations identified

of a formal structure to facilitate joint decision making by the two agencies. To overcome these obstacles and deficiencies, the Street inquiry made recommendations for improving inter-agency communication at the operational level such as attaching ASIO officers to the joint counter-terrorism teams in Sydney and Melbourne and the development of a joint operations protocol. Another initiative arising from the inquiry is the development of guidelines outlining the role of the Commonwealth Director of Public Prosecutions in counter-terrorism investigations.

In addition to the above, there was also the matter of the lack of accountability of the AFP and ASIO. In a submission to the recent inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008, conducted by Senate Standing Committee on Legal and Constitutional Affairs[6], the Castan Centre for Human Rights Law at Monash University identified a number of areas where a 'dilution' of the accountability of these agencies had been evident, citing the Haneef and Ul-Haque cases as examples. It also reminded the Senate Committee that in the Ul-Haque case, and as seen above, Justice Adams of the NSW Supreme Court had been highly critical of the conduct both of AFP and of ASIO officers. According to the Castan Centre, the two cases demonstrate that the law enforcement and security agencies need to be held more accountable in exercising their statutory powers. The Senate Committee noted that the Centre's submission 'emphasised that this was not just about protecting human rights, but also about preserving agencies' integrity' by requiring them to account more fully for the exercise of their powers (SSCLCA 2008: 31).' Similar concerns about human rights protection and accountability moved Mr Petro Georgiou, a Liberal Party backbencher, to introduce a Private Member's Bill into the House of Representatives in March 2008 with the aim of appointing an Independent Reviewer of Australia's terrorism laws similar to the UK independent reviewer who had been appointed in 2000 (Lord Carlile of Berriew) (Georgiou 2008 and 2008a). The Government used its majority in the House to block debate on the Bill.

5 Assessing the impact of the Haneef and Ul-Haque cases

In its submission to the Clarke inquiry, the Gilbert + Tobin Centre for Public Law at the University of New South Wales noted that the fear of persecution in Australia's Muslim communities engendered by the anti-terrorism legislation, a fear brought to light by the SLRC and PJCIS reviews, had been exacerbated by the manner in which the government, the AFP and ASIO had conducted the Haneef affair. The corrosive effect of the authorities' conduct of the affair had not only been felt in Muslim communities, for it had also given rise to 'deep cynicism' across the wider Australian community. This was a worrying development in a security climate in

by Justice Michael Adams.

[6] For clarification, the main purpose of the Amendment Bill is 'to extend the sunset provisions that provide exemptions from the prohibition against listening to or copying communications passing over a telecommunications system' which were due to expire on the 13th of June this year.

which the Australian people should be able to have trust in their Government and confidence in its ability accurately to assess the level of threat faced by the country. As the submission pointed out:

> The promotion of social cohesion is integral to stopping terrorism in its tracks. More specifically, the cooperation and good relations between police and intelligence agencies and Australian Muslims is a crucial resource in unearthing and preventing potential terrorists. The ability under a range of Australian laws to pursue Dr Haneef over nothing more than his familial association with terrorism plotters in the United Kingdom understandably alarmed those in close-knit ethnic communities and must seriously have impacted on efforts to reassure Australia's Muslims they have nothing to fear from these laws (Lynch, McGarrity, Williams 2008; a similar point is made, but not as forcefully, in the Law Council of Australia's submission to the inquiry (LCA 2008: 23)).

The problem here is with the catch-all nature of the terrorism organisation offences that have been inserted into the Criminal Code, in particular, those relating to recklessly associating with, recklessly providing resources to and recklessly helping an organisation to carry out a terrorist act. Because these offences did not precisely target 'unambiguous criminal activity', a repeat of the Haneef affair was almost inevitable (for detailed analysis of the terrorism organisation and other terrorism offences see Lynch, MacDonald and Williams (eds.) 2007 and Lynch and Williams 2006). Not only did excessively wide criminal laws of this type create opportunities for 'executive overreach', they could well make Australia less secure 'by fostering cynicism and division in the community, and wasting police resources on investigations that are trivial or baseless (Lynch, McGarrity, Williams 2008).' For these reasons Australia can ill afford to have a repeat of the Haneef affair. Hopefully, this is a consideration which will move Attorney-General McLelland and his Government quickly to set about removing the ambiguities, sloppy definitions and catch-all offences that are contained in Australia's anti-terrorism laws. The legislative appointment of an Independent Reviewer of the anti-terrorism legislation would be an important first step in this direction.

The Ul-Haque case gives rise to similar concerns and misgivings to those arising from the Haneef case, but ones that are more directly focused on the actions of the law enforcement and security authorities than on the behaviour of the Government itself. In the Ul-Haque case, the AFP and ASIO were found by Justice Adams to have behaved in a manner which was improper and oppressive, rendering the records of interview with Ul-Haque they had obtained inadmissible as evidence in a criminal trial. It is to say the least alarming that these two agencies, which should be committed to upholding the rule of law and protecting Australia's national security, feel that they can behave in such a reckless and unlawful manner. But it is even more frightening when ASIO officers commit criminal offences in a desperate and misguided attempt to collect enough evidence to have an accused but still innocent person convicted of criminal offences. This is a clear perversion of due process and the rule of law which undermines rather than preserves the AFP's and ASIO'S integrity and reputation in the wider community.

Just as importantly, such behaviour undermines national security. Even if national security is taken to mean nothing more than the security of the nation from terrorist attack, then it is clear that in genuine terrorism cases the national security of Australia would be gravely weakened were the AFP and ASIO to behave in the same manner as they did in the Ul-Haque affair. But, if national security is to mean more than just the protection of the country from terrorist attack, and include as it should the security and liberty of the person from arbitrary arrest and detention and similar abuses of state power, then these two agencies have already effectively undermined Australia's national security (see Rix 2008 for an elaboration of some of these points).

Notwithstanding the outrageous and completely unacceptable behaviour of the AFP and ASIO in the Haneef and Ul-Haque cases, they cannot take all the blame for the abuses of due process and human rights that occurred. The lack of accountability of these agencies for the exercise of their statutory powers is just one element, however important, of the political climate in which these abuses were allowed to take place. Other elements have only recently come to light.

In a case being heard before the Commonwealth Administrative Appeals Tribunal (AAT) in Brisbane it has been revealed that representatives of the Department of Prime Minister and Cabinet (then John Howard's department) met with Immigration and Foreign Affairs officials on 4 July 2007 (Haneef was arrested on 2 July) to discuss how the Haneef case should be handled. The action in the AAT was launched by lawyers representing Mohamed Haneef in a bid to assist the Clarke inquiry to procure documents relating to the case. The inquiry does not itself have the power to compel Government departments and agencies to provide it with documents. One of the documents which the action seeks to procure is the options paper developed by the various department represented at the meeting on 4 July which set out the possible courses of action that could be taken should the APF lay charges against Haneef (who was charged on 14 July). According to Haneef's lawyers, 'the involvement of Mr Howard's department raised the possibility the former prime minister may have colluded with his immigration minister to create a political storm similar to the Tampa controversy which helped the Coalition win the 2001 election (*The Australian*, 17 June 2008)'. It is almost inconceivable that Mr Howard was not briefed by his senior advisors about the meeting. While most of the requested documents had been provided to Mr Haneef's legal team, about 15 documents which Government lawyers claim either it is not in the public interest to release or are exempt from freedom of information legislation have yet to be released. The Immigration Department has so far refused to release the options paper.

The political climate created by the former Government's anti-terrorism legislation not only emboldened the AFP and ASIO to perpetrate abuses of due process and human rights. It also sanctioned representatives of Government departments to meet and agree on what could be done in the event that Dr Haneef was charged with committing a terrorist offence. What could be done in this event was clearly to be determined by what would put the Government in the best possible light and cause it the least amount of damage in the public's eyes. Whether or not the Prime Minister and Immigration Minister were directly involved, and whether or not they knew of the meeting, is really not the point. The more important point is the politicisation of the public service and the corruption of its capacity for providing independent advice to the Howard Government or any other that might have succeeded it.

6 Conclusion

The Haneef and Ul-Haque cases are both important for they reveal how a crude association of Islam with terrorism, an important element of the political climate created by the Howard Government's anti-terrorism legislation, permitted the AFP and ASIO to perpetrate abuses of due process and human rights. And at the very time when social cohesion, Australia's best defence against terrorist violence, is most required the political climate and the abuses it has allowed have sowed the seeds of division, suspicion and cynicism in the Australian community. But their importance goes further than even these compelling considerations suggest. These two cases also reveal how easily Australia's national security can be endangered by the two agencies when they are not subject to a strict accountability regime. If they were to behave in the same way in genuine terrorism cases as they did in the Ul-Haque affair then Australia's national security would be in grave danger in the sense that it would not be secure from terrorist attack. But if national security means more than the protection of the country from terrorist attack, and include also the security and liberty of the person from arbitrary arrest and detention, then Australia's national security has already been undermined. Moreover, the politicisation of the public service has seriously compromised its capacity for providing independent advice to government. Thus far, the Rudd Government has shown little inclination to escape the legacy of its predecessor. It can only be hoped that as it grows in maturity and self-confidence it will become more inclined to do so. Australia's national security depends on it.

References

ABC 2007 'Errors lead to dropping of Haneef charge' (July 27), viewed 20 June 2008, <http://www.abc.net.au/news/stories/2007/07/27/1990249.htm>

ABC 2008 'Lawyers question powers of Haneef inquiry, viewed 30 April 2008, <http://www.abc.net.au/news/stories/2008/04/30/2231639.htm?site=goldcoast>

Aly, W 2007 'Muslim Communities: Their Voice in Australia's Terrorism Laws and Policies' in Andrew Lynch, Edwin MacDonald and George Williams (eds.), *Law and Liberty in the War on Terror*, Federation Press, Leichhardt NSW, pp. 198-210.

The Australian 2008 'Howard's office involved in Haneef case days after arrest', 17 June

Australian Government n.d. Listing of Terrorist Organisations, viewed 3 July 2008,<http://www.nationalsecurity.gov.au/>

Georgiou, P 2008 Independent Reviewer of Terrorism Laws Bill 2008, First Reading, viewed 20 June 2008, <http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=2797453&TABLE=HANSARDR&TARGET=>

Georgiou, P 2008a Independent Reviewer of Terrorism Laws Bill 2008: A Bill for an Act to appoint an independent reviewer of terrorism laws, and for related purposes, viewed 20 June 2008, < http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/Bills/Linked/17030806.pdf>

Law Council of Australia (LCA) 2008 Clarke Inquiry into the case of Dr Mohamed Haneef (16 May), viewed 23 May 2008, <http://www.nswbar.asn.au/circulars/haneef.pdf>

Lynch, A 2007 'Should Australia's Muslim Communities really be concerned about Anti-Terrorism Laws?', *Human Rights Defender*, vol. 16, issue 2, pp. 7-9.

Lynch, A, Williams, G 2006 *What Price Security? Taking Stock of Australia's Anti-Terrorism Laws*, University of New South Wales Press.

Lynch, A, MacDonald, E, Williams, G (eds) 2007 *Law and Liberty in the War on Terror*, Federation Press, Leichhardt NSW.

Lynch, A, McGarritty, N, Williams, G 2008 Clarke Inquiry into the case of Dr Mohamed Haneef [Gilbert + Tobin Centre of Public Law submission to Clarke Inquiry] (16 May), viewed 23 May 2008, <http://www.gtcentre.unsw.edu.au/news/docs/Clark_Inquiry_Haneef.pdf>

Maley, P 2008 'Few public hearings in Haneef inquiry, *The Australian*, 30 April.

Maley, P 2008 'Haneef witnesses risk civil lawsuits', *The Australian*, 1 May.

Maley, P, O'Brien, N 2008 'Australian Federal Police in firing line over hidden Dr Mohamed Haneef evidence', *The Australian*, 14 March.

McKenna, M 2008 'AFP "withheld" Mohamed Haneef evidence', *The Australian*, 30 April

McLelland, R 2007 Address to Security in Government Conference (7th December), viewed 15 February 2008, <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~i000071207+Security+In+Government+-+Canberra.pdf/$file/i000071207+Security+In+Government+-+Canberra.pdf>

McLelland, R 2008 Transcript of Clarke Inquiry into Haneef Case, viewed 14 March 2008, <http://www.attorneygeneral.gov.au/www/ministers/robertmc.nsf/Page/Transcripts_2008_13March2008-ClarkeInquiryintotheHaneefCase>

McLelland, R 2008a Press Conference: Same-sex discrimination; Clarkeinquiry, 30 April, viewed 1 May 2008, <http://www.abc.net.au/news/stories/2008/04/30/2231639.htm?site=goldcoast>

Marr, D 2008 'Police ignored strong evidence showing Haneef's innocence', *The Sydney Morning Herald*, 14 April.

New South Wales Supreme Court 2007 [R v Ul-Haque [2007] NSWSC 1251], 5 November 2007, viewed 1 May 2008, http://www.lawlink.nsw.gov.au/scjudgments/2007nswsc.sf

O'Brien, N 2008 'Share intelligence or repeat Ul-Haque debacle', *The Australian*, 28 February.

Peatling, S 2008 'Haneef free to work as appeal dropped', *The Sydney Morning Herald*, 17 January.

Parliamentary Joint Committee on Intelligence and Security (PJCIS) 2006 Review of Security and Counter Terrorism Legislation, viewed 21 March 2008, <http://www.aph.gov.au/house/committee/pjcis/securityleg/report/report.pdf

Rix, M 2006 'Australia's Anti-Terrorism Legislation: The National Security State and the Community Legal Sector', *Prometheus*, vol. 24, no. 4, pp. 429-439.

Rix, M 2008 'Australia and the "War against Terrorism": Terrorism, National Security and Human Rights', *Crimes and Misdemeanours*, 2/1, pp. 40-59.

Security Legislation Review Committee (SLRC) 2006 Report of Security Legislation Review Committee, viewed 21 March 2008, <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~SLRC+Report-+Version+for+15+June+2006[1].pdf/$file/SLRC+Report-+Version+for+15+June+2006[1].pdf >

Senate Standing Committee on Legal and Constitutional Affairs (SSCLCA) 2008 Telecommunications (Interception and Access) Amendment Bill 2008, viewed 20 June 2008, <http://www.aph.gov.au/senate/committee/legcon_ctte/ti_2008/report/report.pdf>

UN n.d. 'The Consolidated List established and maintained by the 1267 Committee with respect to Al Qaida, Usama Bin Laden, and the Taliban and other individuals, groups, undertakings and entities associated with them', viewed 4 April 2008 and previously and subsequently for updates, <http://www.un.org/sc/committees/1267/consolist.shtml.)>

10

Technology in foreign policy and national security: a factor, a tool, and a mediator

Lucy Resnyansky

Research Scientist, Defence Science and Technology Organisation

Abstract

In this paper, I present a social scientist vision of the changing and transforming role of technology in the areas such as security, counter-terrorism, and political stability. The nature of the problems emerging in relation to the changing technology-security landscape stimulates a growing trend towards interdisciplinary research and a dialogue between researchers and practitioners. It is necessary to identify the roles played by different kinds of technology within specific activity areas. A systematic overview and analysis of existing research on this issue can help construct a holistic picture of technology within the rapidly changing defence/foreign policy and security landscape, which is a necessary prerequisite for the development of recommendations to government and security agencies regarding the most effective and efficient use of technologies. Focusing on Information and Communications Technologies (ICTs), this paper develops a conceptual framework to analyse the roles that particular ICTs may play within specific kinds of security/defence activities and settings. This paper makes a distinction between the following roles: (1) technology as a factor of social and political life; (2) technology as a tool of information extraction and analysis; and (3) technology as a mediator between the areas of knowledge production (research) and knowledge consumption (application of research in practice), focusing on modelling and simulation tools. It is argued that the last issue deserves particular attention due to the government's orientation towards evidence-based policy and the interdisciplinary nature of contemporary defence and security problems.

Keywords: technology, information and communications technologies (icts), government, modelling, interdisciplinary, practice

> Like art and religion, technology is an integrated part of a culture (Rivers 2005, p. 567).

1 Introduction

Technology has penetrated the social fabric and security practices so deeply that it is sometimes used without any reflection on its implications. This does not allow the practitioners (as well as the developers of new technologies) to fully realise the transformative potential of technology and is thus seriously limiting the exploitation of this potential. In order to develop a concrete course of action, measures of effectiveness, and a sound government policy regarding the R&D priorities, acknowledging and highlighting the important role of technology in contemporary security and defence areas is not enough. It is necessary to identify the roles played by different kinds of technology within specific activity areas. A systematic overview and analysis of existing research on this issue can help construct a holistic picture of technology within the rapidly changing defence/foreign policy and security landscape, which is a necessary prerequisite for the development of recommendations to government and security agencies regarding the most effective and efficient use of technologies. In this paper, I present a social scientist vision of the changing and transforming role of technology in the areas such as security, counter-terrorism, and political stability. The overall purpose of this paper is to contribute to the integration of social science knowledge into the area of defence, security and technology research.

2 The role of technology in defence and security

The role of technology in contemporary defence and security is discussed within areas such as foreign policy studies, intelligence research, information science, computational social science, and terrorism research. These discussions often focus on technological aspects of new weapons or applications and aim to understand how new technologies are changing the nature of threats and the threatening actors, how they may effect security practices, and what is their social and cultural impacts (Bennett and Resnyansky 2006; Michael and Michael 2006, 2007; Resnyansky 2006; Weiss 2005). The nature of the problems emerging in relation to the changing technology-security landscape stimulates a growing trend towards interdisciplinary research and a dialogue between scientists, social researchers and practitioners (Resnyansky 2007a, 2008; Turnley 2005; Zevallos 2007). Forums are organised that highlight the importance of bringing together the efforts of engineers, computational scientists, social scientists, and practitioners such as intelligence analysts, defence managers and politicians and government officials (Nau and Wilkenfeld 2007; *Threat anticipation: Social science methods and models* 2005). These forums focus on the new applications and methods, practitioners' needs and concerns, and new possibilities and challenges that technology may bring to practice.

Focusing on Information and Communications Technologies (ICTs), this paper suggests a conceptual framework to analyse the roles that particular ICTs may play within specific kinds of security/defence activities and settings. This paper makes a distinction between the following roles: (1) technology as a *factor* of social and political life, focusing on the phenomenon of blogging; (2) technology as a *tool* of information extraction and analysis; and (3) technology as a *mediator* between the areas of knowledge production (research) and knowledge consumption (application of research in practice). It is argued that the last issue deserves particular attention due to the government's orientation towards evidence-based policy and the interdisciplinary nature of contemporary defence and security problems.

3 Technology as a factor of social and political life: blogging

The Internet (blogging, computer-supported social networks, graphical virtual reality environments, etc) attracts the attention of social researchers both as a source of information and opinions and as a new factor affecting socialisation and community building (Herring 2002; Perlmutter 2008, Resnyansky 2007b). Bloggers use the technology (the Internet) as a means to create new social spaces in which social identities and communities are created and transformed, ideas emerge and are disseminated, and patterns of social interaction and political behaviour are (re)produced. It is difficult to understand the role of blogging as a factor of contemporary political life if we focus only on the content of posts or try to measure their potential impact on political life by asking if bloggers are a representative slice of the population. Features of blogging such as hyperlinking structure make them a revolutionary form of political discourse and a new form of voluntary associations of individuals (Perlmutter 2008). Therefore, in order to understand the role of technology as a factor in contemporary life and, in particular, the impact of blogging on the proliferation of democracy and the level of political violence, the technological aspects of blogging need to be taken into account.

4 Technology as a tool: information extraction

This section outlines those studies that highlight the role of technology as a tool, focusing on information search, data mining, etc. A range of computational techniques, approaches and tools is outlined, distinguishing between the following two kinds of tools: tools for getting data on media and public opinion such as computational applications enabling the user to analyse opinion intensity on a particular topic; and tools developed for information extraction from *open source data* – in particular, news websites, blogs, newsgroups, social network sites, virtual worlds, online games and videogames. The latter kind of computational applications enable the user to answer questions regarding the rules that may govern group behaviour (e.g., a group's engagement in political violence); to get detailed information about specific groups in different parts of the world; to find information about violent events defined in terms of attributes such as victims, perpetrators, location, time, and method or weapons used; and to obtain data on particular groups' attitudes and motivations (Albanese and Subrahmanian 2007).

The information extraction tools enable the user to find huge amounts of information. The next issue is how can this information be used? In the process of being used in practice, data/information has to be transformed, which enhances the chances of it being distorted or lost, over-generalised, pushed beyond limits, and applied uncritically or incorrectly (see, e.g., Tufte 2003). Scientifically rigorous knowledge, once having been transferred to the area of practice, may lose its rigor and meaning. Modelling tools may help the practitioners solve this problem. Below, I elaborate on the concept of modelling tools as mediators in decision-making and analytical processes.

5 Technology as a mediator: modelling

The mainstream explanation for why modelling tools are needed focuses on the nature of the object of analysis. According to this view, the modelling tools are needed due to the increasing complexity and uncertainty of the contemporary world (Cioffi-Revilla and O'Brien 2007). These tools help analysts explore different cultures and situations and answer specific questions such as why the production of poppies in Afghanistan has increased during a certain period and what actions can be undertaken in order to stop this trend (Sliva et al 2007). They can be used to simulate such processes as the effects of information campaigns (Wragg 2006) or political identity formation (Ozik et al 2007) and to train to communicate effectively in cross-cultural interaction (Miller et al 2007). Modelling tools can help practitioners develop scenarios of possible events and actions (Falzon 2006). More importantly, they can help practitioners to critically reflect upon their own assumptions, to clarify their questions and purposes, and to better formulate their information needs (Resnyansky 2008).

Practices are socioculturally and historically specific kinds of activities conducted within concrete institutional settings and affected by current political and ideological situations as well as by the availability of resources, individual biases, preferences, tacit assumptions, and so on (Schatzki et al 2001). Therefore, it may be useful for the practitioners to have tools that can alert them to those biases and encourage them to reflect upon their assumptions. This may be quite successfully done by using modelling tools because they enable the analyst to experiment with different conceptual frameworks and explore different scenarios. In order to develop tools that could support such a critical reflexive thinking, their development needs to be an interdisciplinary enterprise informed as much, or at the first place, by social science as by computational science or engineering.

In the information age, practices need to be turned into scientifically saturated activity. This can be significantly facilitated through the use of modelling tools. Modelling may become one of the most effective ways in which social sciences can be used within contemporary practices of government analysis, policy development, and decision making. The practitioners need knowledge that would be compact yet whose scientific rigor would remain intact.They need knowledge that enables them to develop better situation awareness and understand the effects of their own and others' actions rather than knowledge that would increase the level of uncertainty – the usual outcome of information overload. Practitioners need knowledge that enables them to process information in an effective and purposeful way rather than to spend an ever increasing amount of time on information hunting and gathering. They need knowledge that can help them restore the whole picture from disconnected and fragmented data and understand what kind of additional data/information they may need. They need technologies that use mathematical techniques to find hidden patterns of behaviour in large datasets, and technologies that enable them to analyse that behaviour.

To sum up, practitioners need knowledge and technologies that enable them to 'intensify' their activity of transforming information into meaning and action. In order to address this demand, social science knowledge needs to be given to the practitioners not only in the traditional form such as journal publications or reports but also in the form of 'thinking instruments' such as modelling tools. Apart from the possibility to process and analyse large sets of data, another feature of models as a technology mediating the use of data/information is that they enable the user to explore different scenarios, including purely hypothetical ones. This feature is particularly important for the development of the preventive-constructive strategy of counter-terrorist and security activity because it can help the practitioners develop a better understanding of the effects of possible political decisions and actions.

6 Conclusion

This paper has identified the roles of the ICTs within the national security area and has shown a need for a qualitative change in the current practices of using (analysing and representing) information. It has argued that modelling is a technology that can potentially contribute to a more rapid and efficient movement towards evidence based policy in public administration. In order to take into account the role of ICTs as a factor of contemporary political and social life, to use the technological advantages in the area of information search and processing, to use the information effectively and efficiently and not to be overwhelmed by its quantity and diversity – it is necessary to develop an interdisciplinary perspective bringing together the social science knowledge and the technological knowledge. Modelling tools seem to be a promising means for a more intensive integration of social science knowledge in security practice and political decision making. Modelling tools can represent knowledge in a compact yet theoretically grounded and 'easy-to-use' way, which increases their role as mediators between theory and practice.The modelling technologies can, therefore, fruitfully contribute to the work of contemporary government and security agencies. Due to the conceptual frameworks embodied in those models, these tools can enable practitioners to critically approach the chaotic world of information with more rigor.

References

Albanese, M & Subrahmanian,VS 2007, 'T-REX: A system for automated cultural information extraction', in *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics,* ed D Nau and J Wilkenfeld, AAAI Press, Menlo Park, California, pp. 2-8.

Bennett, P & Resnyansky, L 2006, 'How the concept of ethnicity can inform our understanding of the potential impact of security-related technology upon work practices and society', in *Recent advances in security technology: Proceedings of the 2006 RNSA Security Technology Conference*, eds P Mendis, J Lai and E Dawson, Canberra, pp. 143-158.

Cioffi-Revilla, C & O'Brien, SP 2007, 'Computational analysis in US Foreign and Defence Policy', in *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics,* ed D Nau and J Wilkenfeld, AAAI Press, Menlo Park, California, pp. 26-36.

Falzon, L 2006, 'Social modelling in support of planning and intelligence', in *11th International Command and Control research and Technology Symposium*, Cambridge, UK, <http://www.dodccrp.org/events/11th_ICCRTS/html/papers/114.pdf>.

Herring, SC 2002, ''Computer-mediated communication on the Internet', in *Annual review of information science and technology,* vol. 36, ed B Cronin, Information Today, Medford, New Jersey, pp. 109-167.

Michael, MG & Michael, K 2006, 'National security: The social implications of the politics of transparency', *Prometheus*, vol. 24, no. 4, pp. 359-363.

Michael, MG & Michael, K 2007, 'A note on überveillance', in *From dataveillance to überveillance and the realpolitik of the transparent society (Workshop on the social implications of national security)*, eds K Michael and MG Michael, University of Wollongong, NSW, pp. 9-26.

Miller, CA, Wu, P & Funk, HB 2007, 'A computational approach to etiquette and politeness: validation experiments', in *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics,* ed D Nau and J Wilkenfeld, AAAI Press, Menlo Park, California, pp. 57-65.

Nau, D & Wilkenfeld, J eds 2007 *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics*, AAAI Press, Menlo Park, California.

Ozik, J, Sallach, DL, & Macal, CM 2007, 'Identity in agent-based models: issues and applications', in *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics,* ed D Nau and J Wilkenfeld, AAAI Press, Menlo Park, California, pp. 66-72.

Perlmutter, DD 2008, *Blogwars*, Oxford University Press.

Resnyansky, L 2006 'Conceptualisation of terrorism in modelling tools: critical reflexive approach', *Prometheus*, vol. 24, no. 4, pp. 441-447.

Resnyansky, L 2007a, *Integration of social sciences in terrorism modelling: issues, problems and recommendations*. DSTO-TR-1955, (U), *Commonwealth of Australia,* <http://www.dsto.defence.gov.au/publications/5099/DSTO-TR-1955.pdf>.

Resnyansky, L 2007b, 'The Internet as a communication medium and a social space: a social constructivist approach to the use of open data', in *From dataveillance to überveillance and the realpolitik of the transparent society (Workshop on the social implications of national security)*, eds K Michael and MG Michael, University of Wollongong, NSW, pp. 147-168.

Resnyansky, L 2008, 'Social modelling as an interdisciplinary research practice', *IEEE Intelligent Systems: Special Issue on Computational Cultural Dynamics*, Jul/Aug (in print).

Rivers, TJ 2005, 'An introduction to the metaphysics of technology', *Technology in Society*, vol. 27, pp. 551-574.

Schatzki, TR, Knorr Cetina K & Von Savigny, E eds 2001, *The practice turn in contemporary theory*, Routledge, London.

Sliva, A, Samari, G, Martinez, MV & Subrahmanian, VS 2007, 'SOMA Models of the behaviours of stakeholders in the Afghan drug economy: a preliminary report', in *ICCCD 2007 – Proceedings of the First International Conference on Computational Cultural Dynamics,* ed D Nau and J Wilkenfeld, AAAI Press, Menlo Park, California, pp. 78-85.

Threat anticipation: Social science methods and models 2005, The Joint Threat Anticipation Center Workshop, April 7-9, The University of Chicago, <http://jtac.uchicago.edu/conferences/05/>.

Tufte, ER 2003, *The cognitive style of PowerPoint*, Connecticut Graphics Press.

Turnley, J 2005, *Validation issues in computational social simulation,* <http://hcs.ucla.edu/lake-arrowhead-2005/HCS2005_JessicaTurnley2.pdf>.

Weiss, C 2005, 'Science, technology and international relations', *Technology in Society*, vol. 27, pp. 295-313.

Wragg, T 2006, *Modelling of the effects of information campaigns using agent-based simulation*, DSTO-TR-1853, (U), Commonwealth of Australia,
<http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/4405/1/DSTO-TR-1853%20PR.pdf>.

Zevallos, Z 2007, 'Sociology as "other": Representing sociological knowledge within a national security context', in *Public sociologies: Lessons and trans-Tasman comparisons: TASA/SAANZ 2007 Joint Conference Proceedings* [CD-ROM], eds B Curtis, S Matthewman and T McIntosh, University of Auckland, Auckland, 9 pages.

11

National Security and the Misology-Misanthropy Paradox of Technology

George Mickhail

Senior Lecturer, School of Accounting and Finance, University of Wollongong
Professeur des Universites Invité, IAE, Université d'Orleans, France

Abstract

The evolution of computing did not only result in the disengagement of the populace from its technological complexity, but also their submission to the divine ability of 'scientists', who understand the mathematical complexity of information technologies. Socrates argued that both *'misanthropy'* and *'misology'* stem from 'faith' placed in unreliable people and unsound arguments. Such misplaced faith in surveillance technologies and their protractors, for example, often results in disengagement from debate, which to Socrates was the antithesis to truth and wisdom. This paper explores how society is opting out of debate through the machinations of a *neoconservative credo* that purports *reason.* Under the guise of freedom and democracy, such dogma often exploit the public disorientation following massive collective shocks to achieve control, by imposing *economic shock therapy* to affect change. The resulting profiteering bubble of few private hands appropriating public wealth, are often accompanied by exploding debts. The threat of a disenfranchised populace left outside the 'profiteering bubble', prompts the need for aggressive surveillance. This paper concludes that deifying scientific faith and the degeneration of rationality into subservience to commercial interests have resulted in the rise of a fundamentalist brand of global capitalism, that thrive on the corporatisation of national security, and which is giving rise to a new security world order.

Keywords: Misology, Misanthropy, privacy, surveillance, national security

> We've arranged a global civilization in which most crucial elements profoundly depend on science and technology. We have also arranged things so that almost no one understands science and technology. This is a prescription for disaster. We might get away with it for a while, but sooner or later this combustible mixture of ignorance and power is going to blow up in our faces... I worry that, especially as the Millennium edges nearer, pseudoscience and superstition will seem year by year more tempting, the siren song of unreason more sonorous and attractive. Where have we heard it before? Whenever our ethnic or national prejudices are aroused, in times of scarcity, during challenges to national self-esteem or nerve, when we agonize about our diminished cosmic place and purpose, or when fanaticism is bubbling up around us - then, habits of thought familiar from ages past reach for the controls. The candle flame gutters. Its little pool of light trembles. Darkness gathers. The demons begin to stir (Sagan 1996:32).

1 Introduction

Mathematical logic, which is at the heart of information technology, spread to other disciplines, such as: finance and economics - producing a series of esoteric formulae for manipulating algebraic symbols linking premise to conclusion. Whilst the majority of people may not understand such *mathematical-based* disciplines, they still place much faith in the *divine* ability of 'scientists' and 'economists' who understand the mathematical complexity of information technology.

Idolising information technology contributes to what Socrates referred to as '*misology'* and *'misanthropy'*. Misanthropy comes from having faith in people, such as: politicians, who turn out making a decision to implement a new surveillance technology on false pretences. Misology comes from relying on unsound surveillance information. Eventually, both would make us sceptical to believe that anyone or any information can be trusted. Socrates understood such propensity in people disillusioned with their world, to disengage from debate when it was for him the ultimate road to truth and wisdom (Harris 2008).

This paper draws upon Socrates idea, in how society is opting out of debating issues that threaten its very existence, by the exploitative machinations of the *'economic shock therapy' credo* that purports *reason*. The neoconservative doctrine espouses such fundamentalist credo with the purported promises of more freedom and democracy. For over three decades, Milton Friedman and his apostles had *dictated* this dogma globally during many a time of crisis, because they understood very well that the public's disorientation following massive collective shocks, such as: wars, terrorist attacks or natural disasters, can be used to achieve control by imposing economic shock therapy, to affect real change from the failed social welfare doctrine.

The resulting global profiteering bubbles, due to the huge transfers of public wealth to fewer private hands were not only accompanied by exploding debts, but also with aggressive nationalism that justifies bottomless spending on security. The overshadowing threat of a disenfranchised populace left outside the 'profiteering bubbles', prompts the need by the evolving corporatist states for aggressive surveillance, mass incarceration and shrinking civil liberties and often, though not always, torture.

This paper explores three challenges facing our increasingly fearful society: (a) the deifying of scientific faith and the degeneration of rationality, (b) the rise of "mauvais" capitalism and its shock doctrine, and (c) the evolving national security culture. Those contestable ideas will be debated to inform our understanding of the corporatisation of national security.

2 Scientific faith and the degeneration of rationality

Aristotle's old age dilemma, to understand what is it that humans do when they reason, had dejected into confusion due to the competing views of science, pseudo-science and religious belief. Computational technologies yield no understanding when they utilise arcane formulae for processing algebraic symbols that link premise to conclusion. As a matter of fact, very few of us who believe in gravity, or ocean tides or the four seasons as 'scientific facts' would be able to explain 'rationally' why such beliefs merit credence. The mathematical complexity of 'proof' of those facts prohibits most of us from even pondering a 'scientific' explanation, but we sure have 'trust' for those smart scientists who can provide such an explanation. Fundamentally, then, 'science' has become a matter of faith to most of us, in no less a way than belief in the divine.

The evolution of institutions of higher learning and disciplines on such a mass scale over the past fifty years, had only contributed to the degeneration of 'rational inquiry' into a much feeble synonym for what is considered 'reasonable'. Harris (2008) argues that "reasonable, in turn was allowed to mean *able to give reasons*. And the problem with that - as any fool can see - is that any fool can find reasons for foolishness". Such folly had only downgraded such institutions of higher learning into mere 'factories' producing *en masse* graduates, who can barely even give plausible reasons of their own understanding of their discipline – and all is in the interests of supposedly serving the market place.

The corporatist devaluation of reason had not only left educational institutions presiding over a chaos of claims that lack any common 'rational' ground for devoting resources to their pursuit, but also left 'scientifically' illiterate populations. Seventy-five percent of adults failed a National Science Foundation survey, which had 10 questions, eight of which were simple pretty easy true-false or multiple choice questions (Scientific News 1996).

It was not a surprise that the lack of a workforce that is capable of understanding the scientific thought processes, as well as general knowledge had left high-tech and biotechnology companies no option but to leave Silicon Valley and California. Indeed scientific illiteracy plagues not only the USA but also the rest of the world.

The populace votes and decides about critical scientific issues, such as: global warming or energy resources or water supplies, which affect each and every one of us without any understanding of science. However, those decisions should be scientific, not political or economic ones.

3 "Mauvais" capitalism and its shock doctrine

The unholy alliance between the Agora (economic or market space) and the Pnyx (political space), had seen the rise of a neoconservative doctrine that espouses exploitative machinations of an *'economic shock therapy' credo,* with the promise of more freedom and democracy (Mickhail 2007:177). Milton Friedman, its chief architect, understood very well that the public's disorientation following massive collective shocks, such as: wars, terrorist attacks or natural disasters, can be used to achieve control by imposing economic shock therapy, to affect real change from the failed social welfare doctrine.

Naomi Klein (2007:7) argues that it was Milton Friedman who introduced economic shock therapy to Chile when he advised General Augusto Pinochet on economic reforms in 1973 following the aftermath of his violent coup, and when the country was reeling from hyperinflation. The profiteering bubble had an 83% increase in their income, due to the huge 50% cut in public spending and transferring it over to them. The exploding debts left 45% of the population in poverty, but that was accompanied with aggressive nationalism that justified Pinochet's bottomless spending on security.

Friedman believed that "the speed, suddenness and scope of the economic shifts would provoke psychological reactions in the public that facilitate the adjustment" to those necessary reforms. Meanwhile, anyone who did not adjust was met with the full force of the security apparatus, with mass incarcerations (80,000 approximately) and torture (50,000 approximately) – let alone the ones that simply disappeared (70,000 approximately).

In 1980, Ronald Reagan forged ahead with Friedman's economic shock doctrine in reforming the U.S. government and liberalising the financial markets. At the end of his second term, and according to the Federal Reserve, in 1990 the richest 1% owned 40% of its wealth and the richest 20% owned 80% of America - the greatest level of inequality among all rich nations, and the worst in U.S. history since the roaring 1920s.

In the UK, Thatcher was quick to capitalise on the surge in her popularity following the Falklands war victory in 1982. She privatized gas, steel, airlines, and telecommunications, while declaring an open war on the unions, which resulted in tripling unemployment and a 100% increase in the number of the poor.

In Russia, Yeltsin's ambitious "shock therapy" privatisation, was too sudden for Russia to adapt, especially when Western-style banking or corporate rules did not exist. Kampfner (2007) argues that, "Yeltsin did it partly because Russia was broke, partly because he was intoxicated by the end of the Cold War and gullible towards many of the Western economic advisers who had invaded the Kremlin...” In 1993, he sent in the tanks to abolish a parliament that was in defiance of his extreme economic reform. The Parliament burned down with hundreds killed, the opposition arrested, 72 million impoverished and 17 new billionaires created.

The terrorist attacks on the USA in 2001, prompted a privatised war on terror with US spy agencies outsourcing 70% of their budgets to private contractors. But, it was not until 2003, when the Friedman ideology became official U.S. policy in Iraq, thirty years after it was first introduced in Chile – with the largest privatisation of a war in modern history. The common themes of the ideology, were in full enactment when the Iraqi ‘government’ was forced to privatise 200 corporations, the mass incarcerations and the Abou Gharib torture chambers, while hundreds of thousands killed and 4 million people displaced.

The Tsunami disaster in 2004 was one natural disaster that truly galvanised the compassion of the world, but this did not stop the profiteering entrepreneurs in Sri Lanka, where 35,000 died and one million people were displaced, to quickly claim the coastline and get the Sri Lankan government to forbid the fishing villages from being rebuilt by the sea.

Unfortunately, there are so many more examples of this fundamentalist model of Capitalism, which had found attentive audiences in the South American continent, the Middle East and some other parts of the world – where the same corrupt scenario is repeated over and over again.

Authoritarian Communism is forever tainted by the real-world laboratories of Stalin’s gulags and Mao’s re-education camps, but how about the socio-economic experimentation of the neoconservative crusaders to liberate the global financial market? Klein (2007:20) rhetorically asks why all those violent coups and wars to bring pro-corporate regimes had never been treated as Capitalist crimes?

4 An evolving national security culture

Security has become a central focus of social, economic and political initiatives. The OECD (2008), for example, had launched in 2007 an *‘in-country security system reform consultations’*, to ensure that the benefits from development assistance are not reversed by the outbreak of violent conflict. It even encourages the development of a ‘*culture of security’* mindset, to respond to the threats and vulnerabilities of information and communication technologies.

The security frenzy clutching our world raises age-old questions regarding *dissent, resistance and autonomy* – especially, that security *per se* is not bound by ideology: Communist China, Al-Qaeda and the U.S.A. are all alike in maintaining strict security arrangements. The French theorist Paul Virilio (1977:47) recognised this frenzied obsession with security when he coined the term “Dromology” from “Dromos” the Greek word to race, to describe how speed restructures society in favour of what moves fast to dominate that which is slower;

> ... whoever controls the territory possesses it. Possession of territory is

> not primarily about laws and contracts, but first and foremost a matter of movement and circulation...

He argues that a dromological state of crisis results in a culture obsessed with security and speed; on who can protect themselves best and fastest, or in other words, a technological arms race. This presented global capital with a new opportunity, namely: investment in technological production of weapons, security tools and security provision.

The composite experiences of security in a modern society are not only institutional, but also a personal subjective experience. The complexity of personal feelings of fear and safety intensifies with anti-terror security warnings, for example, plastered around train stations and billboards, "if you see something, say something", and breeds anxiety or ontological insecurity (Sennett 2006:161). It is the fear of what will happen even if no disaster looms. It is also referred to as free-floating, to indicate that someone keeps worrying even if s/he has nothing to fear in a specific situation.

Ulrich Beck (1992:129) recognised that ontological insecurity is due to our heightened awareness of risk in society, when he divided modern civilization into pre-industrial, industrial, and a "global risk society" suggesting that today we feel powerless to minimise those risks. Lasch (1984:23) described our mental state of existence to cope with this 'insecure' world, as a 'survivalist mentality'. In a world hijacked by fear and impending catastrophe, individual survival requires safety and being risk averse, which ingrains passivity as a desired state of existence, while dissent becomes a security concern.

David Garland (2001:139) predicts a future, where our control - through surveillance - culture will provide an 'iron cage' for us all, and a dark age of fear that serves the informational *'datalords'* controlling the security zones. In the USA, the Global Positioning System (GPS) technology enabled the possibility of 'virtual prisons' where there are more than 2 million people in mostly privatised prisons and two executions taking place every week. Europe's prison population is growing faster than ever, as are the numbers of surveillance cameras on city streets, such as with the quarter of a million surveillance cameras in London alone.

Surveillance technology commonly perceived in terms of privacy has a more sinister side, in terms of the socio-economic and political 'sorting and exclusion' discrimination. In the past, Orwellian and Foucauldian perspectives provided a largely centralized understanding of surveillance, but new technologies and the networked social organisation, has given rise to a loose and flowing *rhizomatic* set of processes, rather than a centrally controlled and coordinated system (Deleuze et al. 1980:31). The controlling centre, in this networked decentralized system, has become Occult, which "is not occupied by a known leader or a clear ideology" (Debord 1997:54).

One must ask if the evolving hegemony of security technology is due to a *networked* security-industrial complex on a global scale that threatens to polarise the world along a profiteering bubble and a controlled pacified populace – under the guise of an international security threat, such as the war on terror. If so, then are we witnessing the rise of a new world order propelled by the polarising effect of militarising information and telecommunication technologies?

5 Conclusion

This paper outlined three challenges facing our ontologically insecure society, when discussing some of the issues associated with surveillance technology and national security. Firstly, the deifying of scientific faith is problematic, because the *unintended effect* of this misplaced faith in technology, is disengagement from trying to understand the effect of the technology on our lives, and often results in the pacified submission to the divine ability of the scientific faithful.

Secondly, the exploitative machinations of the neoconservative 'shock economic therapy' credo, that purports more freedom and democracy. They *imposed* their dogma globally on a disoriented public, following massive collective shocks, to affect real change from the failed social welfare doctrine. The resulting profiteering bubble, due to the huge transfers of public wealth to few private hands were not only accompanied by exploding debt, but also with aggressive nationalism that justified bottomless spending on security. The threat of a disenfranchised populace left outside the 'profiteering bubble', prompted the need for aggressive surveillance.

Thirdly, an evolving global security culture had intensified our ontological insecurities. To cope with this 'insecure' world, we adopt a 'survivalist mentality' seeking safety, which implicitly ingrains passivity. In contrast to this desired state of existence, dissent, resistance and autonomy became security concerns that warranted surveillance and control on an unprecedented scale.

In conclusion, the discussion of those challenges brings two points to the fore: (a) a new economy of fear that fuels an emerging security culture, and (b) an intensified ontological insecurity that fuels the need for more security. The paradox of security technology is that its supply can never satisfy the 'self-consuming passion' for its demand. The new global economy (Glyn 2006: 133) with its dynamic change, from fixed geopolitical conflicts, to a constantly changing war on terror, ensures that our demand for security is continually reinvented, where the supply of fear and security are continually changing, so that they would never get used up.

References

Beck, U 1992, *Risk Society: Towards a New Modernity*, Sage, London, UK.

Debord, G 1997, *Revolutionary*, Len Bracken, Feral House, UK.

Deleuze, G and Guattari, F 1980, *A Thousand Plateaus*, trsl.: Brian Massumi, Minnesota University Press, USA.

Garland, D 2001, *The Culture of Control: Crime and Social Order in Contemporary Society*, University of Chicago Press and Oxford University Press, USA.

Glyn, A 2007, *Capitalism Unleashed: Finance, Globalization, and Welfare*, Oxford University Press, UK.

Harris, R 2008, *The Decline of Reason*, viewed 15 May 2008, <http://www.timeshighereducation.co.uk/story.asp?storyCode=401875&sectioncode=26>

Kampfner, J 2007, *Yeltsin brought out Russia's best and worst*, viewed 2 July 2008, <http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2007/04/24/do2401.xml>

Lasch, C 1984, *The Minimal Self: Psychic Survival in Troubled Times,* W.W. Norton & Company, New York, USA.

Mickhail, G 2007, The Agora-Pnyx Paradox, in From Dataveillance to Überveillance and the *Realpolitik* of the Transparent Society, eds. Michael, K. and Michael, K., University of Wollongong Press, Australia.

OECD 2008, Conflict and Peace, viewed 19 June 2008, <http://www.oecd.org/about/0,3347,en_2649_34567_1_1_1_1_1,00.html>

Sagan, C 1996, *The Demon-Haunted World: Science as a Candle in the Dark*, Random House, New York, USA.

Scientific News 1996, *Adults score low in science literacy - results of National Science Foundation study*, viewed on 15 June 2008, <http://findarticles.com/p/articles/mi_m1200/is_n23_v149/ai_18385355>

Sennett, R 2006, *The Culture of the New Capitalism*, Yale University Press, New Haven, USA.

Virilio, P 1977, *Speed and Politics: An Essay on Dromology*, Semiotext(e), New York, USA.

12

The social impact of national security technologies: ePassports, E911 and mobile alerts

Holly Tootell

Lecturer, School of Information Systems and Technology, University of Wollongong

Abstract

This paper explores the adoption of emerging technologies for the purposes of national security. The three technologies chosen were ePassports, E911 and mobile alerts. The study uses a content analysis methodology drawing on popular media documentation to extract the major social and technological impacts of the technologies on citizens as they were reported. The findings of the study indicate that reactions to the three technologies differed. ePassports were considered vastly different to E911 and mobile alerting predominantly because they were seen to be a controlling technology, whereas E911 and mobile alerting were viewed to be about safety and emergency response.

Keywords: radio-frequency identification (RFID), E911, mobile alerting, national security

1 Introduction

The purpose of this paper is to explore the coverage of three technologies being used for national security applications. The concepts of terrorism, security, privacy and liberty are factors that can be shaped by the media in respect to events of national security significance. This paper examines three technologies being used for terrorism response, natural disasters and epidemics. Location-based technologies fulfil an important role in emergency management. Emergency management involves looking at the entire spectrum of emergency needs including prevention, protection and response. In Australia, Emergency Management Australia (EMA) is the government body responsible for emergency management. It is situated in the federal Attorney-General's Department (EMA 2006). In the US, the equivalent body is known as the Federal Emergency Management Agency (FEMA), and is part of the Department of Homeland Security. The common objective of emergency management bodies such as this is to provide a comprehensive strategy to reduce the loss of life and property and protect the respective country from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by coordinating with all agencies in an emergency management system of preparedness, protection, response, recovery, and mitigation (FEMA 2007). Through the analysis presented in this paper, the attitudes towards three of these technologies will be explored. The technologies that have been chosen include: RFID passports (ePassports), the United States-based E911 service and mobile alerting in emergency situations.

2 Data Collection

The data used in this paper is derived from articles retrieved from a number of online databases (Proquest5000, ACM Digital Library, IEEE Explore and Factiva. Each of the databases are international, multidisciplinary databases that incorporate a wide variety of sources including academic journals, newspapers, newswires and industry publications. This variety of sources ensured that the technicalities of the concepts which are not often covered in mainstream media would be included.

Each of these databases was searched for articles relating to the deployment of each of the three technologies using the relevant terms shown in Table 1. Articles relating to the financial status of the company were included in many of the searches because of the impact that one or more national security events have had on the developer or technology partners behind the deployment.

Table 1 Technology search terms

Technology	Search term
RFID passports	(RFID passports) or (epassport)
E911	(E911)
Mobile alerting	(emergency alert) and (SARS) (SMS or mobile or cell) and (emergency or alert)

3 ePassport for National Security

The US Department of Homeland Security has pushed for a worldwide standard for enhanced machine readable passports since September 11. A part of this initiative is the proposal to include RFID chips in all passports. One of the key problems with the inclusion of an RFID chip is that the passport holder will be "continuously broadcasting their name, nationality, age, address and whatever else is on the RFID chip" Schneier (2004). Any receiving device would be able to read the data. Proponents of the technology claim it is the most suitable technology for the task, in preference to a contact smart card, because of advantages including faster processing at customs checks and increasing the difficulty of forging or altering the document. Other countries promoting this approach include Australia and the UK, who have been encouraged by the US initiative to have compatible and conforming systems.

3.1 Data Analysis

The primary theme identified through the content analysis was technology (Table 2). In many of the articles, the potential of the ePassport technology is identified and is followed by discussion of the risks it poses (Leach 2004; Ledlow 2005). Neumann and Weinstein (2006) identify this issue in a more general context, and in a much less negative light than Leach (2004) and Ledlow (2005). The potential of the technology, described by Leach (2004) was to "create a more secure travel document". In light of this though are the opinions of those who see a potential mismatch in agenda between government, businesses and the public. Michael and Michael (2006, p.361) address this theme noting that the influence of media and government policy have significant sway on public opinion.

Table 2 ePassport themes

Concept	Discussion themes
technology	Considers the impact of the RFID chips, from their potential to impact on the public and achieve security.
data	The collection of information and the potential of tracking, and identification through the use of RFID chips.
risk	This theme represents the context (war and terrorist) within which this technology solution has been offered.
privacy	Privacy is of particular interest in respect to government use of information.
systems	This theme represents the players in this technology: business, people, and world.
chips	RFID-enabled passports will have a chip. In this context the idea of personal application, digital technology, and the ability to read the data are a focus.

The interplay between these actors (government, business and the public) is picked up in the observation that:

> Consumer privacy groups have grown in strength this year almost as fast as radio frequency identification technology deployments at businesses and governments (Albrecht 2005).

Glover (2005) is steadfast in his position on the technologies being combined at the risk of obliteration of "traditional ideas of personal privacy". This theme ties closely to surveillance of individuals. Hoversten (2004), Amoore and Goede (2005) and Archer and Salazar (2005) consider the issue of surveillance through the RFID technology being used to track consumer behaviour. With a tone of resignation, the authors believe that it will become an accepted part of life because of the pervasive requirements of the technology in its application. They also note that the practice of surveillance is enabled and made easier through the development of RFID technology. It must be noted that many still argue that RFID is not a tracking technology. Passive tags cannot be used to track, but active tags can be used for tracking purposes (O'Connor 2006).

The impact of RFID technology is being closely monitored through privacy advocacy groups (Albrecht and McIntyre 2005; Tebo 2006) who are encouraging the development and safeguard of legislation to protect consumers. Albrecht (2005) takes a strong position arguing that the current technology-centric attitudes are creating a problem for future generations in being able to define and subsequently defend the notion of privacy. What is apparent in this content analysis is that the dominant attitudes in terms of risk to privacy are negative. Technology-positive attitudes are overshadowed. In the post-September 11 climate, although there is unease for security on both a personal and a national level, the impact of proposed measures to address these security concerns is being given serious consideration.

> What scares me is you have people developing RFID technology, spending hundred of millions of dollars, who are looking at the rest of us and saying, risk, there's no risk. As a result they're not taking any precautions to protect us down the road. Our children's and grandchildren's generation will look back and history will judge us based us on how we handle this threat (Albrecht 2005).

It is clear from the data that privacy and security of information is paramount. In the US experience, the perceived premature deployment of RFID technology resulted in an overwhelming 98.5% of 2335 survey participants responding negatively to the idea (Hoffman 2006). Of these, 2019 respondents listed security and privacy as their top concern. The flow-on effect of this is that the government has had to validate the privacy and security concerns of civil libertarians and security experts, who claim that the government is ill-prepared to deal with the issues raised by the technology (Gonsalves 2005; Rockwell 2006). Sullivan (2005) is also concerned by the issue of premature deployment of the RFID technology because technology developers are ignoring the risks and are not incorporating sufficient concern for future impacts of the technology.

Further to the technology-based concerns is the issue of 'skimming' from distances greater than first thought possible, which presents another privacy concern (Lipton 2005). The technology perspective also raises concern regarding the heavy reliance by governments on increasingly sophisticated technology solutions (Amoore and De Goede 2005).

Arguments raised by civil libertarians often tend toward extremist or worst-case scenarios which directly contribute to the perception of risk and fear. The American Civil Liberties Union suggests that RFID readers could be used by terrorists to identify US citizens as they walk down the street (Gardner 2005). Albrecht (2005) is quite pessimistic in stating that:

> RFID could put us and our information at the mercy of global corporations and government bureaucracies and strip away the last shreds of privacy we have left.

From a national security perspective, there is strong evidence to support the swing towards more control and power in border control. Kliment (2006) puts forward that "the US has tried to use technology to balance the competing claims of border security, individual privacy and international commerce". McHale (2005), Biba (2005) and Loftus et al. (2006) bring to light the perceived dichotomy between privacy and security.

McHale (2005) quotes vice president of Civitas Group, Rick Gordon, as claiming that "it is possible to control the borders thoroughly through technology, but political considerations such as the right to privacy can get in the way". Biba (2005) weighs up the benefits of faster and more secure border entry, but at the cost of personal privacy. Soppera and Burbridge (2005) and Loftus et al. (2006) report the necessity of dealing with privacy and security concerns at the outset of the technology deployment to "reduce the costs of dealing with these later".

Table 3 ePassport ranked list of concepts

technology, security, chips, information, data, systems, privacy, tags, cards, government, U.S., people, personal, risk, track, read, biometric, identity, industry, company, number, digital, world, public, potential, war, terrorist, business, money, surveillance

Table 3 is a ranked list of concepts from the content analysis. In the ranked list risk is not as prominent as the issue of *privacy*. *Privacy* has direct relationships to the data and information that is potentially collected from the systems, whereas *risk* is considered as a pervasive concern which is not linked to one major issue. Interestingly, the concept of *surveillance* is the lowest ranked term. There is no direct link between the issue of *privacy* and the collection of *information*. However, it most certainly forms part of the wider concept of the risk of the technology.

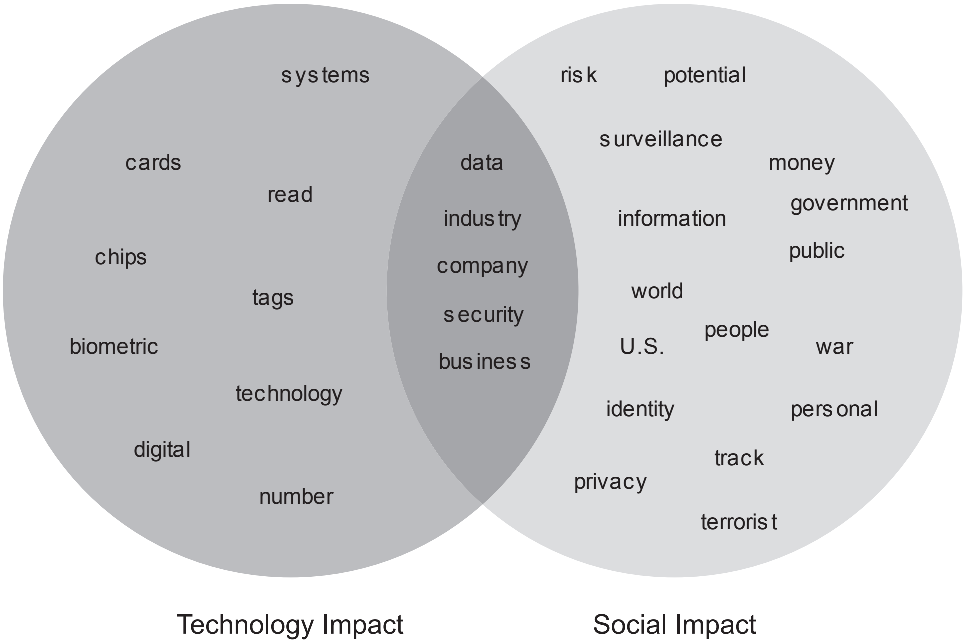


Diagram 1 Technology and social impact of ePassports

In Diagram 1, the concepts from Table 3 have been categorised as technology impact or social impact. In the data collected, there is a greater emphasis on the social impact of this technology. This reflects the media coverage focus on the threat and fear associated with the September 11 attacks. By focusing on the fear, the potential impact of the technology attracts less attention. With the implementation of the ePassport technology as a response to the September 11 attacks, it is expected that this technology will receive relatively little attention. Its introduction was portrayed as a necessary development to prevent a similar attack occurring.

4 E911 for emergency services

E911 (Enhanced 911) is a location technology supported by the US Federal Communications Commission (FCC). Prior to 1996, the service had been available to wired telephony users. The mobile equivalent enables mobile phones to process 911 emergency calls and emergency services to locate the caller's phone number and geographic position of the caller (Dawson et al. 2007, p.4). Prior to the E911 proposal, only a subscriber's carrier was able to handle the call. The new ruling meant that all 911 calls from mobile phones were to be handled by any available service provider. There were two phases to E911. The first, in 1998, required that the phone number be identified and location of the signal tower (cell) is accurate to within a mile. Phase II, in 2001, required mobile phone companies conducting business in the US to offer either handset- or network-based location detection functionality so that "two-thirds of emergency calls received require the location of the individual to be accurate to within 50 metres, and 95 per cent of calls to within 150 metres" (Michael 2004).

4.1 Data analysis

The primary themes identified in the E911 data are shown in Table 3. The concept of location is central to the E911 debate. Wireless and systems refer to the technology focus in the implementation of this scheme. Closely related to location is the issue of privacy. Minor issues raised in the source material refer to signal and state. The signal concept is related to the technology focus of wireless and systems. State refers to the role the FCC and whole government has had in the implementation of the E911 initiative.

Table 3 E911 themes

Concept	Discussion Issues
location	Considers the technology in terms of determining location through signals, and bases. It also considers the impact of application and the role of phone providers.
wireless	This theme is concerned with the emergency communications process through calls and carriers.
privacy	Although a larger issue, this theme is specifically focused on privacy in relation to the companies participating in the E911 scheme.
systems	This theme brings together considerations of data and reliability.
signal	Technology focused theme centres on position, strength in relation to signals.
state	The concern of this theme is on the role of the states in effectively supporting and implementing the E911 initiative.

Much of the media coverage is optimistic regarding the use of the technology as an emergency location identification technology. Behr (2001) has identified the main concern of the technology as the potential of commercial interest in the collected information, separate from the safety uses. He goes on to report that "61 percent said they would be concerned if businesses had access to the information" (Behr 2001). The impact and probability of this is reported by Gold (2000) on mobile provider Sprint, already planning to use the "Qualcomm-supplied GPS-assisted wireless location technology for calls other than E911 ones". Seltzer (2005) identifies a different perspective on the role of the vendors using the E911 equipment for other purposes, being quick to point out that the vendors "are anxious not to get into the middle of such matters and would probably be happy to require user consent before recording and using any location data" even though this secondary use may provide a way of recompensing the expenditure to upgrade systems to comply with the mandate. Seltzer (2005) succinctly describes this as "a tricky dance of convenience vs. trouble, typical of modern technology".

The privacy concerns regarding E911 revolve around the collection and misuse of stored data. Ross (2004) observes that the government is hesitant to advocate the need for enhanced privacy in regard to the technology, suggesting that "no administration ever would because it wouldn't want to limit its ability to obtain information". There is a definite call for transparency in the data collection and use practices, which Ross (2004) and Smith (2006) both reflect on. Prior to the deployment of the current phases of E911, the issue of privacy in relation to the systems supporting the technology were a concern. Gram (1999) and James (1999) talk about preserving the privacy of a new computer database that links the calling phone number with names and locations. Representatives from privacy advocacy groups have been concerned with the risk of misuse of information for a number of years, including the threat that misuse could be initiated "not only by the government but also by the phone companies themselves" according to Jim Dempsey in James (1999). Maintaining a narrow focus of use of information for specific purposes is one suggested means of overcoming the threat of information misuse. Ross (2004) and Smith (2006) suggest that terrorism is one of the issues where there is a good balance between privacy and the need for law enforcement. They have also put forward that the advancement of technology has provided benefits in terms of safety monitoring and response, but has also increased vulnerabilities in relation to the collection of information.

Table 4 E911 Ranked list of concepts

location, wireless, technology, information, services, systems, emergency, system, phone, E911, service, calls, carriers, mobile, data, FCC, public, provide, state, network, phones, number, cell, GPS, privacy, providers, applications, cellular, companies, industry, access, available, personal, telephone, people, base, communications, signal, meet, position, research, area, infrastructure, case,

The ranking of privacy is interesting to note in Table 4. It is of less concern in the E911 than the ePassport data collection.There is an implication in the reporting of this technology that it is less invasive and pervasive than the ePassport initiative. This may be due to the fact that the E911 service is a pull technology, where users are asking for help. In situations where the E911 service is likely to be requested, the user will be in need of assistance, and not in a position to be too concerned about the implications of the technology.

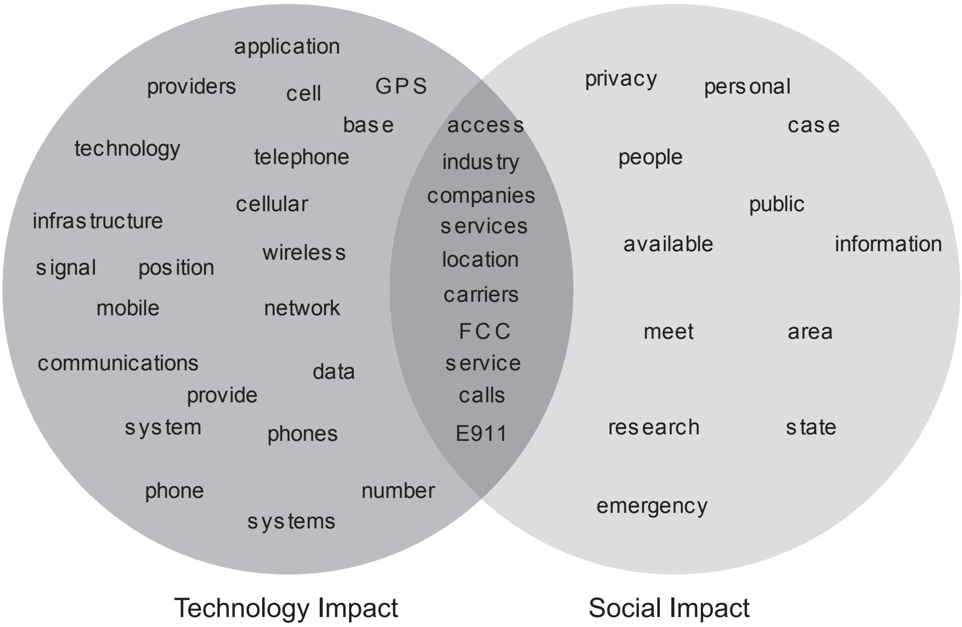


Diagram 2 Technology and social impact of E911

The division between the technology impact and social impact concepts related to E911 (Diagram 2) is more heavily weighted toward the technology than the ePassport initiative division of concepts. More descriptive information about the technology is common in the E911 coverage. As the E911 initiative was developed, it was openly discussed in the newspapers and government, which may account for the greater focus. The overlap in Diagram 2 illustrates the blending of the technology issues and social issues, and is indicative of the interaction between the social impact and the technology development.

5 Mobile Alerting for Commercial Application Based on SARS Outbreak

Mobile alerting allows users of mobile phones to receive messages regarding location-specific information. For everyday use, mobile alerting is a subscription-based service packaged as an add-on to the ordinary payment plan. During the SARS outbreak, Hong Kong mobile phone provider Sunday Telecom, and Singapore-based provider Starhub, had an opt-in service in which subscribers had their phones tracked (Michael and Masters 2006). When the mobile phone came within a one kilometre radius of a reported SARS case, an SMS would be sent to notify of the affected building (Staff 2003). This service can be used for many applications: emergency communications is one example, others include: find a friend services, and location specific restaurant and shopping offers.

5.1 Data Analysis

The primary themes identified in the Mobile Alerting data are shown and described in Table 5. The relationship of these terms provides the structure for the following discussion.

Table 5 Mobile alerting themes

Concept	Discussion issues
people	This theme represents the impact that the SARS outbreak has had on the world. It includes information regarding the spread of the disease.
mobile	The role of companies, services and subscribers is covered in this theme.
services	This concept represents the SMS alerts from a network and patient perspective.
system	It is important to recognise the role of the public health system in managing the global outbreak.
technology	This theme identifies the development of the early warning emergency notification systems.

Mobile alerting technology brings many benefits in emergency alert applications, but a number of issues, including privacy and network infrastructure, are viewed as impediments to fast and complete deployment (Christopher 2006). From a user's perspective, any potential downside to the subscription service is outweighed by the benefits of the location-based warnings, especially those needing to work in affected areas (Wong 2003). The immediate threat of SARS contributed to the popularity of the mobile alerting service. The ease of signing up for the alerts (Lui 2003) and the perceived benefits they delivered meant that the mobile alerting was extremely convenient for users. The convenience of the mobile alerting is also greater than the newspaper service as noted by Wong (2003).

Wickham (2005) identifies a number of logistical considerations of releasing "all-points bulletin for all devices across all carriers within a specific geography". He believes it is an opportunity for government and business to come together to create a workable plan for meeting all requirements addressing the needs of everyone from emergency service providers to customers.

Sunday Communications launched the location-based SARS alert service in Hong Kong. It was designed to alert subscribers when they were within one mile of a building where people have been infected by SARS (Liu 2003; Lui 2003; Ramakrishnan 2003; Spy Blog 2005). From the success of this alerting system, Sunday Communications has gone on to provide other location-based notifications.

The success and acceptance of the SARS mobile alert model has impacted in various areas. Eysenbach (2003) expands the notion, illustrating the idea with remote patient monitoring systems that can be adapted to early warning systems for widespread outbreaks of infectious diseases.

The financial impact of SARS was felt strongly by mobile providers. The decline in roaming revenue due to reduced travel was countered by the increase in call traffic. It was noted that telephone communication was preferred to face-to-face contact during the initial period (Yuk-min 2003; Zuckerman 2003).

Table 6 Mobile alerting ranked list of concepts

Hong_Kong, mobile, people, phone, service, outbreak, system, health, disease, phones, information, world, company, million, government, services, spread, local, SMS, global, public, patients, subscribers, countries, alert, technology, early, reserved, network, emergency

Table 6 is a ranked list of concepts from the content analysis. The focus of these terms is the impact of the technology on people. There is continued emphasis on the impact of the disease outbreak, rather than the specification of the technology. Emergency is the lowest ranked concept. The list of terms shows beyond the initial shock and emergency status of the SARS epidemic to the ongoing influence it has had on the population it affected. A number of terms refer to the international impact of mobile alerting: people, world, global, and countries.

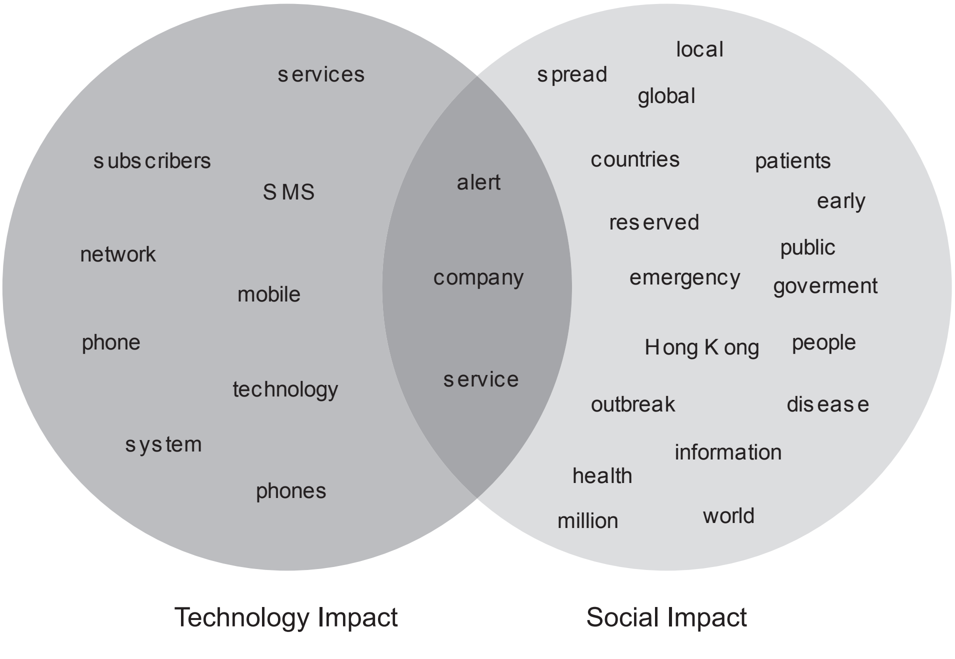


Diagram 3 Technology and social impact of mobile alerting

The division between technology impact and social impact concepts related to mobile alerting (Diagram 3) is more heavily weighted toward the social impact than the E911 initiative. This social impact focus aligns with the results of the analysis, which determined a concentration on finding methods to manage the severity of the outbreak and communicating effectively with the population. The effect on health services is reflected strongly in Diagram 3.

6 Reflections on the media coverage of the technology

The technologies examined in this chapter were all created or further developed as a response to a national security event and in many instances, the probability of the same events occurring is minimal, but technology-based solutions were implemented regardless. There is an interesting distinction between the reactions to ePassports, E911 and mobile alerting. E911 and mobile alerting were extensions of existing technologies, where the current development and deployments were a small step from previous use, whereas the ePassport was a new development.

Table 7 News content in the mass media

News Making	Description
Event-driven	The hard core of media content. Events which actually occur and which are reported in a relatively straight-forward way.
Managed	These are 'created' news events, whether for commercial, political or governmental interests.
Media-coloured	News treatments through which events are magnified, distorted or sometimes even invented; moral panics.

In relation to the technologies covered in this paper, a subset of categories has been defined in Table 7. These categories will shape the discussion in the following sections.

6.1 The media reponses to mobile alerting and E911

The 'selling' points for E911 and mobile alerting appealed to the masses due to the likelihood of necessity. Mobile alerting is of particular interest in this respect, because this style of communication has become widely accepted in areas other than emergency response. As it does not require subscribers to change already adopted methods of communication, technology is not an adoption inhibitor. Both E911 and mobile alerting can be considered pull technologies. From this perspective, it is the user who instigates the use of the technology. When this is the case, there is a need perceived by the user to have that service activated. The availability of the technology, and its potential impact on privacy and liberty might still be debated in theory, but at the time of need, basic survival instinct is likely to override these concerns.

The concept of privacy, in relation to mobile alerting, was not listed. This does not rule out privacy as a concern, but it does indicate that privacy concerns are low. The low level of concern may be accounted for by the pre-existing relationships between mobile phone users and the mobile network providers, and related to the description of a pull technology above.

E911 recorded the second-most significant reaction in relation to technology acceptance. The E911 technology was a second phase of development of an existing technology. The September 11 attacks prompted further development of this service, especially in light of the confusion of the emergency response effort. Media reaction to this technology was more explanatory than confrontational in comparison to ePassport. The everyday nature of the technology meant that users did not have to adopt any additional devices or learn any new methods of operation. The invisible integration of E911 into the lives of the American people helped to create interest in the technology without it being considered an intrusion.

In terms of the styles of news making (Table 7), the coverage of both E911 and mobile alerting was predominantly event-driven. A comparison of the discussion themes for both these technologies illustrates this (see Table 8).

Table 8 E911 and mobile alerting concepts vs ePassport concepts

9a	
E911 Concepts	**Mobile Alerting Concepts**
location	people
wireless	mobile
privacy	services
systems	system
signal	technology
state	

9b
ePassport Concepts
technology
data
risk
privacy
systems
chips

The terms listed in Table 8a have more to do with the actors and the components of the technology than the ePassport concepts. Although privacy rates as a concern with regard to E911, the context of it was about company use of information. The context was removed from significant personal concern and can be seen as an argument of concern about company ethics.

6.2 The Media and ePassports

The ePassport initiative was developed as a response to the September 11 attacks. It promised increased security to the holders, but also prompted curiosity as to the effectiveness of it as a preventive measure in the fight against terror. The media coverage of the technology drew on the climate of fear that prevailed in the months following the attack: which classifies the coverage as managed and/or media-coloured. The questioning in the media about privacy, surveillance and tracking played a part in maintaining the 'war on terror' rhetoric. This rhetoric is now beginning to haunt the government.

Unlike the other two technologies, the ePassport is a push technology. The ePassport initiative questioned the intention of the government in relation to its citizens through the media. Consent was not sought from citizens in the US, or countries who have adopted this technology as a standard in order to comply with the US. As a push technology, the ePassport technology required travellers to take additional and different action to their normal course. Push technologies are likely to encounter resistance to adoption because of this. It is the combination of the push technology with the portrayal in the media, through managed stories and media-colouring that contributes to the different perception of the technology by the public.

The concepts identified in Table 8b mostly centre around the application of the technology and it's potential for misuse. The term technology, in relation to ePassport had connotations of mistrust between the public and government. This is different to its use in the mobile alerting context. Each of the ePassport concepts has been tempered by degrees of media-colouring, especially in regard to the creation of moral panic. Marshall and Kingsbury (1996, p.43) refer to Stanley Cohen's (1973, p.9) definition of the term 'moral panic' as,

> A condition, episode, person or group of persons (that) emerges to become defined as a threat to societal values an interests; its nature is presented in a stylised and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people…

Given this definition, the context of the adoption of this technology involved more risk than the other two examples, and tended to include coverage that had more bias toward personal and social impact rather than technology-driven concern. It is important to note that the ePassport does not act in a direct life-saving way as E911 does. This is a technology that provides protection to other travellers 'just' in case you are doing something wrong.

7 Conclusion

The purpose of this paper was to describe the media coverage of three technology applications being used for national security purposes. Each technology was described, and then analysed through the identified concepts. By illustrating the identified concepts in the concept map and the ranked list of concepts, connections could be made with regard to the impact of the technology deployment.

The media can act from many perspectives. The main perspectives identified in this data include the event-driven and media-coloured coverage. These categories help to describe and understand the findings that show the balance between social impact and technology impact. The use of media coverage in this paper to gauge reactions to the technologies has continued to shape the perceptions of interest: privacy, security and liberty.

References

Albrecht, K. 2005, 'Privacy and RFID: Are the tags spy chips?' *TechWeb*, vol.November 3, p.1.

Albrecht, K. & McIntyre, L. 2005, *Spychips: how major corporations and government plan to track your every move with RFID*, Nelson Current, Nashville.

Amoore, L. & De Goede, M. 2005, 'Governance, risk and dataveillance in the war on terror', *Crime, Law and Social Change*, vol.43, no.2-3, p.149.

Archer, Q. & Salazar, G. 2005, 'RFID: a threat to privacy?' *Computer Weekly*, vol.April 5, p.18.

Behr, M. 2001, 'Worried about wireless privacy?' *PC Magazine*.

Biba, E. 2005, 'Biometric passports set to take flight', *PC World.Com*.

Christopher, A. 2006, *Stopping the next SARS with cell phones*, accessed 14 January 2007, http://www.technologyreview.com/Infotech/16161/page2/

Cohen, S. 1973, *Folk Devils and Moral Panics*, Paladin, St Albans.

Dawson, M., Winterbottom, J. & Thomson, M. 2007, *IP Location*, McGraw-Hill, New York.

EMA. 2006, *Australian Government Role in Emergency Management*, accessed 3 May 2007, http://www.ema.gov.au/agd/EMA/emaInternet.nsf/Page/Emergency_Management

Eysenbach, G. 2003, 'SARS and population health technology', *Journal of Medical Internet Research*, vol.5, no.2, p.14.

FEMA. 2007, *About FEMA*, accessed 29 July 2007, http://www.fema.gov/about/index.shtm

Gardner, W.D. 2005, 'E-Passport program rolls out in Singapore', *InformationWeek*, vol.April 11.

Glover, T. 2005, 'The end of privacy is nigh as use of radio chips spread', *Sunday Business*, 29 May, p.1.

Gold, S. (2000) "Privacy storm brewing over mobile phone location tech." *Newsbytes News Network*, accessed 4 March 2006, http://findarticles.com/p/articles/mi_m0NEW/is_2000_Nov_10/ai_66894415

Gonsalves, C. 2005, 'An RFID passport to trouble ', *eWeek*, pp.22-33.

Gram, D. 1999, 'Police push for database access raises privacy concerns', *Associated Press Newswires*, 8 September.

Hoffman, S. (2006) "RFID privacy concerns." *iSeries News*, accessed 2 February 2007, www.systeminetwork.com

Hoversten, P. 2004, 'RFID gets airing in Congress; critics warn of privacy issues', *Aviation Week's Homeland Security & Defense*, vol.3, no.29, p.4.

James, F. 1999, 'Safety versus privacy FCC wants phones to reveal location', *Denver Post*, 13 September, p.F.01.

Kliment, A. 2006, 'US issues new 'E-passport' despite fears on security', *Financial Times*, 10 March, p.3.

Leach, S.L. (2004) "Passports go electronic with new microchip." *Christian Science Monitor*, accessed 14 January 2006, http://www.csmonitor.com/2004/1209/p12s01-stct.html

Ledlow, A. 2005, 'The future of RFID', *Truck News*, vol.25, no.8, p.43.

Lipton, E. 2005, 'Bowing to critics, U.S. plans to alter electronic passports', *New York Times*, 27 April, p.A.21.

Liu, J. 2003, 'China checks mobile messages for SARS rumors', *Reuters Health E-Line*, 13 May.

Loftus, M., Burbank, L., White, M. & Alipio, A. 2006, 'Smart Traveller: your next passport', *National Geographic Traveler*, vol.23, no.2, p.12.

Lui, J. (2003) "Cell phone firm offers SARS alerts." *CNETAsia*, accessed 23 April 2006, http://zdnet.com.com/2100-1103_2-997457.html

Marshall, I. & Kingsbury, D. (1996). Media Realities: The News Media and Power in Australian Society. Melbourne, Addison Wesley Longman Australia Pty Limited.

McHale, J. 2005, 'DHS turns to high tech to control borders', *Military & Aerospace Electronics*, vol.16, no.7, pp.22-26.

Michael, K. 2004, 'Location-based Services- a vehicle for IT&T convergence', in K. Cheng, D. Webb and R. Marsh (eds), *Advances in E-Engineering and Digital Enterprise Technology: Proceedings of the 4th International Conference on E-Engineering and Digital Enterprise* Wiley Publishing Inc., London, pp.467-477.

Michael, K. & Masters, A. 2006, 'Realized applications of positioning technologies in defense intelligence', in H. Abbass and D. Essam (eds), *Applications of Information Systems to Homeland Security and Defense*, Idea Group Publishing, Hershey, pp.196-220.

Michael, M.G. & Michael, K. 2006, 'National Security: The Social Implications of the Politics of Transparency', *Prometheus*, vol.24, no.4, pp.359 - 363.

Neumann, P.G. & Weinstein, L. 2006, 'Risks of RFID', *Communications of the ACM*, vol.49, no.5, p.136.

O'Connor, M. 2006, 'N. H. Reps Approve 'Tracking Device' Bill', *RFID Journal*.

Ramakrishnan, J. 2003, 'Sunday to build on SARS location-based mobile data offering', *WMRC Daily Analysis*, 19 May.

Rockwell, M. 2006, 'RFID hits a bump', *Wireless Week*, vol.12, p.19.

Ross, P. 2004, 'Barr says congress should address E-911 privacy threats', *Communications Daily*, vol.24, no.23 February, p.35.

Schneier, B. 2004, *RFID passports*, accessed 13 August 2006, http://www.schneier.com/blog/archives/2004/10/rfid_passports.html

Selby, N. 2003, 'Location-based services find niche', *International Herald Tribune*, 5 May, p.11.

Seltzer, L. (2005) ""They" Know Where You Are." *eWeek.com*, accessed 3 February 2007, http://www.eweek.com/article2/0,1895,1893642,00.asp

Smith, G. 2006, 'Private eyes are watching you: with the implementation of the E-911 mandate, who will watch every move you make?' *Federal Communications Law Journal*, vol.58, no.3, pp.705-727.

Soppera, A. & Burbridge, T. 2005, 'Wireless identification -- privacy and security', *BT Technology Journal*, vol.23, no.4, p.54.

Spy Blog (2005) "SMS disaster alert and warning systems - don't do it!" *Spy Blog: Watching Them, Watching Us*, http://www.spyblog.org.uk

Staff (2003) "Operator Delivers SARS Updates." *Wireless Week*, accessed 23 April 2006, http://www.wirelessweek.com/article.aspx?id=76506

Sullivan, L. (2005) "Privacy and RFID: are the tags spy chips?" *InformationWeek*, accessed 13 August 2006, http://www.informationweek.com/story/showArticle.jhtml?articleID=173402917

Tebo, M.G. 2006, 'Who's watching the watchers?' *ABA Journal*, vol.92, p.36.

Wickham, R. (2005) "Use SMS & LBS for early warning systems " *Wireless Week*, accessed 12 December 2005, www.wirelessweek.com/toc-archive/2005/20051001.html

Wong, M. 2003, 'Cell phone company offers location-based SARS reports', *Tulsa World*, 22 April, p.E3.

Yuk-min, H. 2003, 'China Mobile expects to generate extra revenue during virus crisis', *South China Morning Post*, 3 May, p.3.

Zuckerman, A. 2003, 'E911: When will trucking and the public see it?' *Transport Topics*, no.3544, p.S6.

13

You are where you have been

Roger Clarke[1] and Marcus Wigan[2]

[1]Principal, XamaX Consultancy Pty Ltd, [2]Professorial Fellow, The University of Melbourne

Abstract

Location is a critical aspect of both privacy and surveillance. A detailed record of locations allows all sorts of other information to be linked together, adding to information about the subject and his or her associates in the same way that a unique identifier allows dataveillance to be expanded so swiftly and extensively. This time by allowing the linking of both the activities and records of many different people together. Location technologies have far outstripped both public awareness and legal and policy attention. Addressing this gap will require careful use of precise language to ensure that unexpected side effects do not occur when this is finally faced up to, and the present paper explores both this essential language and some of the applications and linkages that need addressing. A wider public and policy understanding of the implications of the expanding capacities to track, record and monitor location is an urgent need, as it is very difficult to reverse capacities once integrated into a wide range of commercial, enforcement and intelligence systems – as is already happening.

Keywords: location, GPS, RFID, surveillance, privacy, tracking, retrospective, carbon budget, middleware, anonymity, protocols, geospatial, transport, intelligence, embedded identity

1 Introduction

A decade ago, technologies that could provide information about the location of a motor vehicle, or a computer, or a person, were in their infancy. A wide range of tools are now in use and in prospect, which threaten to strip away another layer of the limited protections that individuals enjoy. While steady moves to identify, trace and record locations of things and animals has long been established, the application to people is now gaining momentum, and requires a reappraisal. An understanding of the landscape of location and tracking technologies, and of the issues that they give rise to, depends on establishing a specialist language that enables meaningful and unambiguous discussion to take place.

Location-based aspects of mobile phones, public transport smart cards and Automatic Numberplate Recognition are used to illustrate the emergent prospective and retrospective issues. The central concern is that the multiplying technologies for real time and retrospective location tracing have advanced far beyond the legal and privacy frameworks that we have in place. In combination with unique identifiers (for people or vehicles) the potential for remarkably intrusive data assembly and use has become a reality that has not been catered for. Neither public expectations not policy exists to handle the social impacts of this wonderfully unobtrusive surveillance technique, and both are necessary if the benefits are to continue to be realised without either significant losses to civil society or a substantial backlash once it becomes known.

Even when appropriate policies and legislative backing have been developed, the confusions between privacy and identity, and what comprises a sufficient yet not enduring identity to preserve privacy will need to be carefully communicated.

This paper commences with a brief overview of key concepts underlying the subsequent discussion. One cluster of relevant concepts comprises real-world entities (particularly humans and vehicles), identities, and pseudonymity and anonymity. A second cluster comprises the concept of location and the process of acquiring it, and the concept and process of tracking.

Building on these ideas, the paper briefly surveys the privacy impacts of location technologies, in order to set the scene for subsequent papers, and to provide a basis for addressing the possibility of privacy protecting middleware for systems currently being developed and deployed. One's location is potentially very sensitive personal data. But the tracking of people's movements both real-time, and retrospectively, lifts the threat to a much higher level and has become a form of function creep that has already become established practice in some quarters.

1.1 Background

Nearly two decades ago Daniel, Webber and Wigan (1990) identified the likely outcomes from the advanced traffic identification, tolling and linkage technologies becoming planning options for operations, and the implications of these location, time and activity specific tracing technologies. Roughly a decade later the sharper issues of more general location data acquisition and integration with other data holding were highlighted by Clarke (1999a), who reviewed location and tracking in what was then still a somewhat simpler world than today. Clarke's paper noted increasing intensity in the collection of transaction data, in the association of personal identifiers with that data, in the retention of that data, and in mining of that data. It also referred to the emergence of spies in people's pockets, wallets and purses (smartcards and cellular mobile phones), and in their cars (toll-road tags, and tagging by car-hire companies, insurers and investigators), and to the integration with other data systems as foreshadowed ten years earlier.

Those technologies are now well-established, and lack any form of consistent- or in some cases even any- regulatory framework. Cellular triangulation and signal-differential techniques, and self-reporting of GPS measurements are also error-prone, but their accuracy and precision appear to be improving. However, Nokia in California has been actively developing methods of movement and traffic monitoring that preserve anonymity, and advocacy for privacy in the emergent location based services via mobile phones is a live and promoted issue in this research team (Jacobsen, 2008).

Radio Frequency Identification (RFID and Near Field Communication (NFC) devices identify and locate chips with reasonable reliability, and, because of their short range, with considerable accuracy. NFC is not widely known. A good source of information on NFC is the industry forum (NFC Forum, 2008), and NFC is increasingly being integrated into mobile phones and used for contactless transactions in various forms of transactions – including public transport. The NFC Forum specifically included credit card companies such as Visa, and is working on device independent intercommunication with a major emphasis of contactless identification applications. Meanwhile, Automatic Number Plate Recognition (ANPR) surveillance of traffic has been introduced with minimal regard for its impact on privacy and freedom, although very recently a Queensland Government enquiry into ANPR recognised it as an issue in the issues paper (Travelsafe, 2007).

For the last four decades, discussions of privacy and surveillance have primarily focussed on the collection and handling of personal data. In effect, the orientation has been towards *'you are what you've transacted with us'*.

The march of information technology has resulted in the scope of the transactions that are being recorded are expanding exponentially, due to the increasing ability to link different data sources- and now to add probabilities of associations from proximity or repeated visits to specific locations, where 'people of interest' might also go. Now organisations in both the public and private sectors are seeking data about where people are, in order to use it - sometimes at least nominally for themselves, but in practice mostly against them or at the very least to pick them out as objects of special interest, be it marketing, tracking, monitoring, or active surveillance. The almost complete absence of data destruction requirements for such implied transaction data means that data about *'where you are now'* is kept, and becomes a trail of *'where you've been'*. Even when there are data retention duration requirements (eg. UK Government (1998) and Canadian Government (2001)), the ability to undertake the fuzzy linkages with people or objects in some proximity to the location sequences traversed can (and probably will in practice) occur. The only protection against such linkages is to design and audit systems accessing location based data, and **demonstrate** that they cannot undertake such tasks (Daniel et al, 1990). Even in cases where there are legislative provisions this will remain a risk – and any occurrence will probably remain unauditable ex-post as well.

The presumption underlying the exploitation of this pool of data is that *'you are where you've been*', and to which we may now add 'the probabilistic associations of others visiting the same locations at various times'. This addition enhances intelligence activities (Michael et al, 2006.) - but does not increase precision in a civil law sense.

The latter is a critical and quantum change in the surveillance capacities, as such associations are (necessarily) probabilistic (or circumstantial) evidence - until unique personal identifiers on both parties are added to the mix. This new expansion of dataveillance techniques moves from the evidence base of current surveillance systems, which are largely compatible with civil law, to the anticipatory and necessarily probabilistic approaches that are the unique domain of intelligence and anti-terrorist operations – which operate on quite different bases for action. This is a major shift, and one that is largely innocuous when done for marketing purposes- but changes the nature of civil society if added to normal civil law and the complementary police approaches to evidence.

2 Concepts of identity, entity, nymity

This section provides an overview of the concepts of identity, entity and nymity. It draws heavily on relevant parts of Clarke (2001, 2004).

The term **'entity'** refers to any item that exists in the real world. It is sufficiently generic to be applicable to a rock, a chair, a motor vehicle, a device with a computer embedded in it, and a human being.

The term **'identity'** refers to a particular presentation of an entity, such as a role that the entity plays in particular circumstances. For example, a motor vehicle is an entity. It may have multiple identities over time, such as taxi and getaway car. A mobile phone is an entity, but it may take up different identities depending on the SIM placed in it. A computer is an entity, but each process that runs on it is capable of being an identity distinct from both the entity and the other identities represented by other processes.

People perform many roles, and most individuals are known by different names in different contexts. In some cases, the intention is dishonourable or criminal; but in most cases the adoption of multiple personae is neither, but rather reflects the diversity of contexts in which they act, including within their family, their workplace(s), their profession, community service and art. In common law countries, people are in no way precluded from using multiple identities or aliases. Actions that take advantage of multiple or situation-specific identities in order to cause harm or circumvent the law are, on the other hand, criminal offences, and there are increasing attempts to limit even the legal use of multiple identities for administrative and enforcement convenience. If this occurs there are many unfortunate consequences (Wigan 2007). These include the stripping of protection through no longer being able to assume a different identity for personal safety reasons for such groups as witnesses, psychologists, victims of family violence and many others.

An identity may be distinguished from other, similar identities through the use of some kind of label or signifier. For example, a SIM card has a SMI-card identifier, a process running in a computer has a process-ID, and a human being has (many) names and codes assigned to them.

Similarly, an entity may be distinguished from other, similar entities through the use of some kind of label or signifier. Even some rocks have names or numbers, motor vehicles have vehicle id numbers (VINs), engine numbers and registration 'numbers', mobile phones have unique numbers associating with housing, Radio Frequency ID (RFID) chips (used in all sorts of transport, logistics and manufacturing process, passports etc) and human beings have biometrics. Given that the term for an item of information that distinguishes an identity is **'identifier'**, it is convenient to refer to an item of information that distinguishes an entity as an **'entifier'**.

An identifier that can be linked to the underlying entity only with considerable difficulty is commonly called a **pseudonym**. If an identifier cannot be linked to an entity at all, then it is usefully called an **'anonym'**. And a term that usefully encompasses both pseudonyms and anonyms is **'nym'**.

Anonymity is a characteristic of Records and Transactions, such that they cannot be associated with any particular entity, whether from the data itself, or by combining it with other data. **Pseudonymity** is a characteristic of Records and Transactions, such that they cannot be associated with any particular entity unless legal, organisational and technical constraints are overcome. And a term that encompasses both anonymity and pseudonymity is **'nymity'**.

The concepts of location and tracking, discussed below, clearly apply to entities. However they may also apply to identities in various circumstances, and hence to **nyms**.

3 Concepts of location and tracking

This section provides an overview of the concepts of location and tracking for geospatial referencing. It draws heavily on relevant parts of Clarke (1999a).

By an entity's location is meant a description of its whereabouts, in relation to other, known objects or reference points. Examples include the following:

- The location of a real estate property may be defined in what geospatial specialists refer to as 'cadastral' terms (in this case the attributes of a specified area with a Lot Number within a Deposited Plan) and/or in geographical terms, commonly as latitude and longitude (i.e. relative to an imaginary grid defined relative to the earth's surface);

- The current location of a person or a vehicle may be defined as being on a named street, at an approximate distance from a named street-corner or outside a numbered or named building;
- The location of a device communicating with a cellular network service may be defined by reference to the location of one or more towers from which the cell is run. The location of devices relative to the tower(s) may be computed by such means as directional sensing, triangulation or differential signal analysis;
- A device that has a global positioning system (GPS) chip-set installed may be able to compute its position on the basis of available satellite signals. In this case, it is expressed in latitude and longitude plus elevation (i.e. relative to mean sea-level). The device may record or self-report that position: GPS is not in itself a surveillance system.
- The 'space' within which an entity's location is tracked is generally physical or geographical. All of the above examples relate to location within physical space. Other kinds of 'space' exist and location within such spaces may be defined in other terms. For example, a location may be virtual, as in the case of a person's successive interactions with a particular organisation. A particularly important example is 'network space'. An IP-address records the location in network space of a software process entity (which necessarily is running in a computer entity).

Location can be ascertained with varying degrees of precision, accuracy and reliability. These are addressed formally in the US Federal Geographic Data Committee (FGDC, 1998) metadata system for geospatial information in addition to other issues in geospatial quality as they are critical factors in location (see also Perusco and Michael, 2005). The location of installed devices such as fixed ATMs and EFT/POS terminals may be quite exact, and reliable. The locations of some EFTPOS (Electronic Funds Transfer at the Point of Sale) terminals (e.g. those in taxis) are much more ambiguous, as are those of small modems, codecs and Ethernet and other network interfacing cards, which may be removed from their recorded location.

Devices such as cellular phones, and portable and hand-held computers, are designed to be mobile, and additional information is needed in order to draw inferences about their location at the time of a particular event. Some kinds of location definition may be limited to a line or cone (e.g. those relying on directional mechanisms), or an area bounded by three or more lines (e.g. those relying on triangulation). However there is a rapid growth in Augmented GPS systems, where GPS is supplemented by additional information of local inputs.

Measures of location may be available with varying degrees of:

Timeliness. By this is meant the lag that occurs between the event, and the availability to a person undertaking surveillance of the transaction data reflecting that event.

By '**tracking**' is meant the plotting of the trail, or sequence of locations, within a space that is followed by an entity over a period of time.

Due to timeliness limitations, data may only be available for **retrospective analysis** of a path that was followed at some time in the past. A **'real-time' trace**, on the other hand, enables the organisation undertaking the surveillance to know where the entity is at any particular point in time, with a degree of precision that may be as vague as a country, or as precise as a suburb, a building, or a set of co-ordinates accurate to within a few metres.

Moreover, a person in possession of a real-time trace is in many circumstances able to infer (as yet only selectively) the subject or object's immediate future path with some degree of confidence (Graham, 2008). The capacity to do this on increasing numbers of designated targets (people of vehicle/objects of interest) is rapidly increasing. However the Microsoft, UC Berkeley and University of Maryland collaborative work program (Hu &Wang, 2005; Jiang et al, 2007), on which Grahams' article is based, also addresses privacy options.

4 Privacy threats in location and tracking

This section provides an overview of the privacy threats inherent in location and tracking. It draws substantially from Clarke (1999a). The threats arise from individual technologies, and the trails that they generate, from compounds of multiple technologies, and from amalgamated and cross-referenced trails captured using multiple technologies and arising in multiple contexts. The human and ethical issues of enhanced location based identification are also addressed by Perusco and Michael (2005). The fundamental concepts of dataveillance and the risks it embodies are examined in Clarke (1988).

Location and tracking technologies give rise to data-collections that disclose a great deal about the movements of entities, and hence about individuals associated with those entities. Given an amount of data about a person's past and present locations, the observer is likely to be able to impute aspects of the person's behaviour and intentions. Given data about multiple people, intersections of many different kinds can be computed, interactions can be inferred, and group behaviour, attitudes and intentions imputed.

Location technologies therefore provide, to parties that have access to the data, the power to make decisions about the entity subject to the surveillance, and hence to exercise control over it. Where the entity is a person, it enables those parties to make determinations, and to take action, for or against that person's interests. These determinations and actions may be based on place(s) where the person is, or place(s) where the person has been, but also on place(s) where the person is not, or has not been. Tracking technologies extend that power to the succession of places the person has been, and also (probabalistically, but in the case of real time monitoring, increasingly accurately) to the place that they appear to be going.

Currently locational data is largely only a by-product of the operations of traffic systems, public transport operators, mobile phone operations, ambulance and courier services, and those actively collecting data from a small sample of people for research purposes. Active monitoring is in place for vehicle theft, high value transactions in transit – or, in the case of operators such as FedEx or UPS, a realtime monitoring through transit points is a user service that they offer for all their identified packets. The ANPR systems in the UK are now connected to the online registration and licensing databases at the Driver and Vehicle Licencing Authority (DVLA), and is in use by police to anticipate the arrival of vehicles and persons of interest travelling along UK motorways. These are simply a few of the growing number of systems and capabilities: the ANPR/DVLA linkage to Police operations is a significant harbinger of what is in store.

The nature and extent of the intrusiveness is dependent on a variety of characteristics of location and tracking technologies. An analysis is provided in Clarke (1999b), encompassing such factors as the intensity of the data collection process, the data quality, data retention and destruction, and data accessibility.

Dangers that are especially apparent include the following:

- **Psychological harm** through embarrassment, loss of control over one's life, and devaluation of the individual, which arises from the knowledge or suspicion that the person is being watched;
- **Social, cultural, scientific and economic harm**, arising from the 'chilling effect' on personal and group behaviour, and especially non-conformist, inventive and innovative behaviour, which arises from the knowledge or suspicion that some or all of the group are being watched. These mechanisms are lucidly covered by Kim (2004);
- **Political and democratic harm**, arising from the 'chilling effect' on personal and group behaviour, and especially the voicing of unpopular opinion, participation in demonstrations, and other forms of political opposition or dissident behaviour, which arises from the knowledge or suspicion that some or all of the group are being watched. On the notion of **'dissidentity'**, see Clarke (2008);
- **Profiling and suspicion-generation**, through the discovery of individuals' behaviour patterns, thereby enabling matching against pre-determined patterns. This can be used by the State in order to generate suspicion, and by the private sector to classify the individual into micro-markets and thereby to manipulate consumer behaviour;
- **Substantially enhanced scope for damaging or embarrassing** (political or personal) disclosures, blackmail and extortion. This has a deleterious effect on democracy, because it reduces the willingness of competent people to participate in political life;
- **A vast increase in 'circumstantial evidence'** for criminal cases, which

might dramatically affect the existing balance through lack of contestability, including the presumption of innocence, and hence increase the incidence of wrongful convictions. This would in turn result in a more credible threat of conviction (including in ambiguous and spurious instances), and hence in increased repression of human behaviour. The much enhanced information asymmetry between individual and the state would then extend not only to detailed records of locations far beyond anyone's possible detailed memory to retain, but also to the assumptions of association from others who may have coincided in the same locations on one or more occasions, this asymmetry is a serious concern as it is largely circumstantial as location records are object related, not person related and not even nym related – unless secured using an injected RFID chip. Some of the governance issues are covered in a companion paper at this meeting (Wigan, 2008);

- **Enhanced visibility of behaviour.** This increases the potential for measures to be taken against individuals, both by agents of the State, and by corporations whose behaviour is impinged upon by the person and actual repression of the readily locatable and traceable individual (Clarke 1988, 1994b.) The focus of public concerns is usually an exercise of power by the State, but these technologies also greatly empower corporations. The capability will be useful in dealing with troublesome opponents, such as competitors, regulators and lobbyists, but also employees, whistleblowers, consumer activists, customers and suppliers. The degree of impact on each individual depends on their psychological profile and needs, and their personal circumstances, in particular what it is that they wish to hide, such as prior misdemeanours, habits, and life-style, or just the details of their personal life. Some categories of individual are in a particularly sensitive position.

'Persons-at-risk' is a useful term for people whose safety and/or state of mind are greatly threatened by the increasing intensity of data-trails, because discovery of their location is likely to be followed by the infliction of harm, or the imposition of pressure designed to repress the person's behaviour. Examples include VIPs, celebrities, notorieties, different-thinkers, victims of domestic violence, people in sensitive occupations such as prison management and psychiatric health care, protected witnesses, and undercover law enforcement and security operatives.

Marketers have an interest in identifying population segments and networks, and in building personal behaviour profiles (e.g. mobile location advertising). So too do intelligence agencies, to identify associated persons in National Security applications.

Legislative bodies are beginning to make such information the basis (which may be by visits to a location) grounds for potential criminal action or enforced restrictions. Recent legislation passed in South Australia (Government of South Australia, 2008) will, when it comes into effect, make a limited number of associations through membership or deemed membership (visits to specific locations being one, if circumstantial, basis for such assignment) a basis for assigning people to a specific group subject to police and possible legal action.

More sinister applications arise because so-called 'counter-terrorism' laws have greatly reduced the controls over data gathering, storage and access, over inferring about where people have been and whose paths people have crossed, and over detention, interrogation and prosecution.

5 Location and tracking technologies

A wide variety of location and tracking technologies exist. They are mostly oriented towards entities, and their effective operation depends on the collection of entifiers (the range of possible encodings of different forms of identity for entities) that distinguish the particular entity and enable transaction data to be reliably associated with the appropriate entity and perhaps with other transactions. Some technologies are relevant to spaces other than physical space (especially net space), and some to identities rather than entities. Many specific instances of location and tracking technologies were catalogued and outlined in Clarke (1999a).

During the intervening decade, a few of these have become noticed by the general public. In particular, there is an increasing appreciation that mobile phones have become not only a personal convenience, but also a spy in the person's pocket, reporting continually the device's presence in a particular cell (and hence continually disclosing its location to an accuracy of 100m to a few km), even when nominally switched off.

Cell-phone location and tracking data is subject to security and some privacy regulation, but most of the features have been designed from an engineering perspective and privacy protections are incidental rather than intrinsic. The protections are subject to very substantial exceptions. The protections have been effectively nullified by extended powers for law enforcement agencies during the long national security extremism phase that followed 11 September 2001 (colloquially referred to as "9/11" in the US-style). The protections are subject to compromise by the increasing prevalence of public-private partnerships, and the vast concessions that Governments are granting for-profit corporations in return for taking over the burden of infrastructure provision and maintenance.

The rapidly developing scenario of locationally-based services (often referred to as LBS) is not without positive examples. The Mountain View based company LoopT (2008a) offers geospatial social networking services, and now deliver location based push advertising with CBS. Clearly aware of the sensitivity of location-linked and sensitive technologies, they have carefully expressed aims to allow users to manage their privacy- (LoopT, 2008b). It remains to be seen if the advertising linkages with CBS will leave this intent untouched. There are no formal controls or standards in this area, and they are clearly needed. CBS Mobile are requiring users to 'opt-in' and CBS intend to deliver advertisements anonymously and not retain any location records.

> 'So far, privacy and technology concerns have held back the prospect of personalized mobile ads from the likes of Starbucks or Barnes & Noble. But using LoopT's GPS-based technology and capitalizing on its relationships with mobile carriers, CBS Mobile wants to make it easier for advertisers to aim promotions at consumers more precisely as they walk by particular stores and restaurants' (New York Times, 2008c).

Clearly, some users are apparently not as sensitive about some location based services as they might be were they fully aware of the cumulative record linking capacities of such services. They will pay for them (Isqbal & Lim, 2007), and their specific consent is needed under European Privacy legislation (Loenen & Zevenbregen, 2007). Pelsys (2008) in South Australia already offers personal tracking via mobile phones as a commercial service for employers to track their staff and even to tale pictures and transfer these back to a monitoring base station as part of the service. It is not clear what freedom – if any – these staff may have to disable or deny the use of such intrusive location based services for their employer, although it is but a small step onwards from the accepted commercial vehicle tracking services already on offer. Such commercial services might indeed in the future be used for personal carbon budgets… or to track the carbon budget usage of an organisations' staff.

The assessments of particular technologies in Clarke (1999a, 1999b) and above are mainly conceptual, and the terms 'locational' etc are now being more clearly framed in specific cases for discussion of privacy and surveillance issues, although the privacy issues are well recognised (Bettini et al, 2005; Ackerman et al, 2003). In order to bring real examples into closer focus, this section adds a few succinct vignettes that illustrate in greater depth some of the specific and highly problematic technologies (and software and management systems) that have rapidly appeared and even more rapidly been applied. Many appear to be subject to almost no meaningful privacy controls, and have extraordinary and highly negative implications for privacy, and for civil liberties and political freedoms more generally.

To position the nature of the concerns and how they might be addressed, a positive and negotiated example is given first.

5.1 Detailed identified trip purpose, location and data collection programs

The use of GPS to track individuals with their full consent to secure transport planning information now has close to a decade of experience, and has become a standard tool of trade. This is perhaps the only area where full knowledge and assent is always secured, and anonymising is part of the protocol. As long ago as 2004, typical mainstream examples and commentary were provided by the US Transport Modeling Improvement Program (TMIP) (Guensler, 2004).

Murakami et al (2004) summarises travel data collected, emphasising how detailed and comprehensive it is compared to household methods, and Guensler (2004) reports result of adding instrumentation to 487 vehicles in 270 households which in addition to trip data report speed and engine operating data in real time via a mobile phone connection. The subjects were sampled randomly and a very large fraction agreed to participate over a substantial period of time.

Specialised high sensitivity personal recording equipment has been developed by several transport data specialists in Australia, such as the Centre for Logistics and Transport at the University of Sydney who has applied it to commercial vehicle data collection (Graves & Figliozzi, 2007). The general area of location based services and security and privacy has been given a further impetus from the augmented GPS systems in the European Union. The GALILEO project (European Commission, 2007) is well known for being planned to provide an alternate set of GPS services, but far less well known for offering augmentation of the GPS data and the list of specific services that will be offered. An encrypted authentication scheme is to be available for navigation services, for example, as well as a structured series of ground GPS augmentation and the EGNOS service provision centres on which third party location based services can be delivered.

> 'The European Geostationary Navigation Overlay Service (EGNOS) is Europe's first venture into satellite navigation. It augments the two military satellite navigation systems now operating, the US GPS and Russian GLONASS systems, and makes them suitable for safety critical applications such as flying aircraft or navigating ships through narrow channels' (European Space Agency, 2007).

This infrastructure is an example of what is possible (Pozzobon et al, 2004) if new technology for linking location-based services with other types of services is planned for **in advance.**

The lesson is that fully informed consent and responsible management can be acceptable, especially when the application is so clearly for the constructive purposes of transport and traffic planning in the area where the vehicle owners live and work. The levels of detail are very fine grained and linked directly to the people and the vehicles and their operating characteristics at any point in time. The difficult issues are those where these conditions are **not** satisfied. These are for far less transparent and agreed purposes, and the management of the data and its subsequent recording, linkage and data mining are not disclosed to those monitored.

Toll roads have often been costed as areas where anonymity is not even provided for. There are many such examples, where privacy policies have only been created under pressure after they have been opened for traffic (CityLink (2002) in Melbourne), or semi-private with release of deidentified information to specified bodies (ConnectEasT, 2006) EastyLink: also in Melbourne Australia), but this need not be the case. The I-408 toll road in Canada has a specific and clearly stated genuinely anonymous mode of payment, demonstrating that it is possible, but is rarely emulated at this level of follow through (407ETR, 2008).

5.2 Automatic Number Plate Recognition (ANPR)

Far from a balanced and considered implementation of ANPR and the associated databases and linkages, the UK has raced ahead to implement and deploy a national ANPR vehicle surveillance scheme.

In March 2005 the Association of Chief Police Officers of the UK demanded [and now have widely operational] a national network of Automatic Number Plate Recognition (ANPR) UK-wide ANPR data capture

> 'utilising police, local authority, Highways Agency, other partner and commercial sector camera, including the integration of the existing town centres and high street cameras, with a National ANPR Data Centre with an operational capacity to process 35 million ANPR reads every day increasing to 50 million by 2008, stored for two years' (Wood, 2006: p 19).

5.3 Public transport smart cards

The Oyster card for public transport in London is a salient example: one of sufficient notoriety that Richard Stallman (2008) – the founder of Open Source – has publicly protested at such an onerous use of Open Source software. 90% of all bus and underground travel in London is now paid for using Oyster RFID cards (Transport for London, 2008), with 12 million cards now in use. There is **no** anonymous method of payment, and the linkages between credit cards and the Oyster travel and timing records are thus unavoidable. The function creep is well established, with extensive police and surveillance access used. The commercial extensions and function creep is now beginning with the re-implemented Linux based software for faster modification and greater flexibility for Transport for London to utilise- promoting iTunes on the Oyster system with new members getting free vouchers.

The Oyster principles are a major influence on the well-overdue (and over cost) MyKi (myki, 2006) transport ticketing system still under development for Melbourne. Although at least some token attention to privacy is indicated on their website, it remains to be seen if it will remain. In the case of MyKi the extended use of the card to other types of purchases is clearly signalled, so the function creep has begun long before the system has even been finalised.

Oyster has progressively become an major tool for general enforcement and surveillance, the function creep that inevitably occurs once an expensive system begins to work well – many different parties press to get the potential (usually privacy invasive) advantages at minimal marginal cost. This persuasive economic dynamic is one that can confidently be expected to occur again and again – unless clearer privacy rules and new enforcement techniques (maybe drawing upon the same locational technologies with the addition of **nyms** and other forms of temporary identification adequate for the purpose and no more).

5.4 Identity variants and location based services

There has been little coherent treatment of the privacy and security aspects of the many and various forms of location based services. A few examples have been given here where they has been recognised as an issue of recognised importance, and some provisions have been made. These provisions are inconsistent, and follow no particular pattern.

GALILEO has provided for encrypted navigational services with a full protocol, but it is up to service creators to decide how to use these facilities, but they are indeed there to be used. There is no equivalent of middleware for location based privacy services, although there are systematic efforts to move towards it by mobile phone manufacturers. For example, Nokia (2008) provides full application programming interfaces to support such facilities for its developers so that GPS augmentation by other data sources can be easily be used to enhance the location determination and location attributes.

Nuanced locational anonymity is not impossible. Beresford & Stanjo (2003) propose and demonstrate the mix zone, a locational extension of techniques developed for anonymous communications. Another example is Priyantha et al (2000) who describe the Cricket location system under sole control of a PDA user.

Microsoft is also one of the organizations working on a range of protocols for privacy (or the choice of its absence) at both a middleware level and an application level. All of these approaches are not focussed on providing a coherent approach to privacy in a location-enabled environment, and do not distinguish between people and objects.

As a result the careful niceties expounded in the early section of this paper where the variations in association type (and indeed duration) of associations between individual entities in a data system are not yet widely recognised.

It is only when the overall privacy design of the system is considered that such provisions become necessary. The Internet Taskforce GEOPRIV initiative (IETF, 2008) is probably one of the most effective (or at least pervasive) places to begin to contribute such fine – but critical- distinctions to the process.

6 Conclusion

Locational technologies have not previously been seen as surveillance devices in common use, and so the controls – or even the need to have any - have been slow to appear.

'*Where you have been*' is not restricted to location, the massive pressure from many different areas of government and commerce to link up existing data collections on people has a special meaning once the locations visited are not only physical but also social and transactional. To this extent locational issues are sensitive in their own right- but the combination of backward integration with other types of data, as well as historical physical locations, allied to social network analysis offers an almost irresistible attraction to many areas of government administration and commercial enterprises.

In this regard the multiplications of connections that result from adding historical or real time locational data has an impact that draws all individuals and their associations into a single tightly closed net: you may be judged not only where you have been, but by who you were there with (or even close to) - and when. This expansion of connections cannot be ignored and entwines all of us with anyone or any group under monitoring for **any** purpose, historically or prospectively, or, as one might put it, '*you are where you have been and… who with and when.*'

Information technology shares a key characteristic with an elephant: it doesn't know how to forget. It needs to be taught how: very quickly - and provably. This is almost certainly an impossible dream, and the best course of action is to focus on four things:

- Secure a layered privacy and record linkage process, supported by widely used middleware to buffer the added sensitivities of linking in locational data.
- Ensure that the duration of associations between nyms, names and objects etc is as brief as is necessary for the transaction, and make this an industry standard.
- To develop policies that articulate clearly that the intermediate associations are neither needed nor kept beyond the transaction in which they are involved. Especially when approximate locations are used to link disparate people or 'objects of interest'.
- To identify ways in which retrospective linkages are not enabled by location based services, as this will moderate the almost inevitable collateral social impacts.

This too may already be impossible to secure, so '*we are where we were* – **and are now likely to be labelled by the characteristics of those who might also pass through the same locations**'.

References

Ackerman, L., Kempf, J. & Miki, T. 2003. '*Wireless location privacy: law and policy in the US, EU and Japan*'. Internet Society Member Briefing at http://www.isoc.org/briefings/015/ accessed 3 July 2008.

Beresford, & Stanjo. 2003. '*Location Privacy in pervasive computing*'. IEEE Pervasive Computing pp. 1536-1268. At http://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf accessed June 29 2008.

Bettini, C., Wang, XS and Jajodia, S. 2005. '*Protecting privacy against location-based personal identification*'. In *Secure Data Management*. Springer Verlag, Berlin. pp. 185-199.

Canadian Government. 2001. '*A guide for businesses and organisations: Your privacy responsibilities: Canada's Personal Information Protection and Electronic Documents Act*' at http://www.privcom.gc.ca/information/guide_e.asp. Accessed 7 July 2008.

CityLink. 2002. '*Citylink Privacy Code*' at www.citylink.com.au/files/Privacy_Code_Dec_02.pdf accessed 21 June 2008.

ConnectEast. 2006.'*privacy policy' at* http://www.eastlink.ca/about/legal/documents/EastLink_Customer_Privacy_Policy-May2006.pdf on 7 July 2008.

Clarke, RA. 1988, *'Information technology and dataveillance',* Communications of the ACM 31(5), 498-512Clarke, RA. 1994, *'Human identification in information systems: Management challenges and public policy issues',* Information Technology & People 7(4), 6-37

Clarke, RA. 1999a, *'Person-location and person-tracking: Technologies, risks and policy implications'*, Proc. 21st Int'l Conf. on Privacy and Personal Data Protection, pp.131-150, Hong Kong, 13-15 September 1999. Revised version in Information Technology & People 14(2), 206-231.

Clarke, RA. 1999b, *'Relevant characteristics of person-location and person-tracking technologies',* Separately-published Appendix to (Clarke 1999a). Xamax Consultancy Pty Ltd, Canberra.

Clarke, RA. 2001, *'Authentication: A sufficiently rich model to enable eBusiness',* Xamax Consultancy Pty Ltd, December 2001, at http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html

Clarke, RA. 2004, *'Identification and authentication fundamentals',* Xamax Consultancy Pty Ltd, May 2004, at http://www.anu.edu.au/people/Roger.Clarke/DV/IdAuthFundas.html

Clarke, RA. 2006, *'What's 'Privacy'?'*, Prepared for a Workshop at the Australian Law Reform Commission on 28 July 2006, at http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html

Clarke, RA. 2007, *'What 'Uberveillance' is, and what to do about it',* Invited Keynote, In K Michael and MG Michael.'*From dataveillance to uberveillance and the realpolitik of the transparent society'*. Proc. 2nd RNSA Workshop on the Social Implications of National Security'. University of Wollongong. pp. 27-60.

Clarke, RA. 2008, *'Dissidentity'*, Xamax Consultancy Pty Ltd, Canberra, at http://www.anu.edu.au/people/Roger.Clarke/DV/Dissidentity.html

Daniel, M., Webber, MJ & Wigan, MR. 1990,'*Social impacts of new technologies for traffic management*', Research Report ARR 184, Australian Road Research Board, Vermont, Victoria.

Eastlink 2008.'Motorway Info'. at http://www.eastlink.com.au/page.aspx?code=MOTORWAY accessed 3 July 2008.

European Commission 2007.'*GALILEO European Satellite Navigation System'*. At http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm accessed 21 June 2008.

European Space Agency 2007.'*The present - EGNOS navigation*'. At http://www.esa.int/esaNA/egnos.html accessed 21 June 2008.

Federal Geographic Data Committee.'*Content standard for digital geospatial metadata (revised June 1998)*'. FGDC-STD-001-1998. Washington, D.C. USA. At http://www.fgdc.gov/metadata/csdgm/ accessed 12 June 2008.

407ETR. 2008.'*Anonymous accounts'* at http://www.407etr.com/Products/transponders_anonym.htm accessed 7 July 2008.

Government of South Australia. 2008. *Serious and organized crime (Control) Act 2008.* At http://www.legislation.sa.gov.au/lz/c/a/serious%20and%20organised%20crime%20(control)%20act%202008/current/2008.13.un.pdf accessed on 6 July 2008.Greaves, SP & Figliozzi, MA. 2007. '*Commercial vehicle tour data collection using passive GPS technology: Issues and potential applications'*. Paper 08-1294. CDRom, Annual General Meeting of the Transportation Research Board, Washington DC.

Graham. F. 2008. '*GPS gadgets can reveal more than your location'.* New Scientist, 3rd June. At http://technology.newscientist.com/article/dn14052-gps-gadgets-can-reveal-more-than-your-location.html accessed 5 June 2008.

Guensler, R. 2004. '*Atlanta's comprehensive travel data collection effort',* TMIP Connection, Spring. p3 at http://tmip.fhwa.dot.gov/clearinghouse/tmip_newsletter/spring04_issue19/spring04_issue19.pdf

Hu, YC, & Wang, HJ. 2005. '*A framework for location privacy in wireless networks'.* At research.microsoft.com/~helenw/papers/sigasia05.pdf accessed 6 July 2008.

Internet Task Force Secretariat, 2008. '*Geographic location/privacy (geopriv)*' at http://www.ietf.org/html.charters/geopriv-charter.html accessed 9 June 2008.

Isqbal, MU & Lim, S. 2007. '*Designing privacy-aware mobility pricing systems based on user perspective*'. Journal of Location Based Services, 4(1), pp. 274-299.

Jacobsen, Q. 2008. '*Location based wireless services in urban areas and mobility',* Volvo Research Foundation Global Workshop, Berkeley, California (Private communication).

Jiang, T., Wang, HJ. & Hu YC. 2007. '*Preserving privacy in wireless LANSs'*. Proc. 5th International Conf. on movile systems, applications and services. San Juan Puerto Rico. ACM. NY. pp 246-257. At http://portal.acm.org/citation.cfm?id=1247689 accessed 8 July 2008.

Kim, MC. 2004. '*Surveillance technology. Privacy and Social Control'*, International Sociology 19(2), 193-213.

Loenen, BV & Zevenbregen, JA. 2007. '*The impacts of European privacy regime of locational technology development'.* Journal of Location Based Services 1(1) pp. 165-178.

LoopT. 2008a. '*LoopT transforms your mobile into a social compass'.* At https://app.loopt.com/loopt/sess/index.aspx accessed 24 June 2008.

LoopT, 2008b. '*Privacy & Security.* At http://www.loopt.com/about/privacy-security%23forparents%23privacy#privacyfeatures accessed 24 June 2008.

Michael, K. McNamee, A. Michael, MG. & Tootell, H. 2006. '*Location-based intelligence- modeling behavior in humans using GPS*'. International Symposium on Technology and Society, 2006. ISTAS 2006. IEEE. At http://ieeexplore.ieee.org/servlet/opac?punumber=4375874 accessed 1 July 2008.

Murakami, E., Taylor, S., Wolf, J., Slavin, H. & Winick, B. 2004. '*GPS applications in transportation planning and modelling',* TMIP Connection, Spring. p.3 at http://tmip.fhwa.dot.gov/clearinghouse/tmip_newsletter/spring04_issue19/spring04_issue19.pdf

myki, 2006. "*myki will be your key to opening Victoria's public transport'.* At http://www.myki.com.au/ accessed 12 June 2008.

New York Times, 2008. At http://www.nytimes.com/2008/02/06/technology/06mobile.html accessed 20 June 2008.

NFC Forum, 2008. At www.nfc-forum.org, accessed 20 June 2008.

Nokia 2008. "*Forum Nokia – driving mobile innovation: Location-Based services'* at www.forum.nokia.com/main.resurces/technologies/location_based_services.htm on 1 July 2008.

PELSYS (2008). '*Pelsys-Tracker: Vehicle tracking/ Personal tracking'*. At http://www.pelsys.com.au/products/tracker/?gclid=CLyc6vSzrZQCFRUYewodKS4PVA accessed 7 July 2008.

Perusco, L. & Michael, K. 2005. '*Humancentric applications of precise location based services'*. IEEE International Conference on e-Business Engineering (ICEBE'05), pp. 409-418.

Poszzobon, O., Williams, C. & Kubik. K. 2004. '*Secure tracking using trusted GNSS receivers and Galileo Authentication Services*'. Journal of Global Positioning Systems 1-2(3), pp. 200-207.

Priyantha, NB, Chakraborty, A. & Balakrishnan, H. 2000. "*The Cricket location-support system'*. Proc. International Conference on Mobile Computing and Networking. ACM NY pp. 32-43.

Stallman, R. 2008. '*Stallman attacks Oyster's 'unethical use of Linux*', Quoted by Judge, P in ZdNet 9 June at http://news.zdnet.co.uk/software/0,1000000121,39431419,00.htm.

Transport for London. 2008. '*What is Oyster?*'. At http://www.tfl.gov.uk/tickets/oysteronline/2732.aspx accessed 31 May 2008.

Travelsafe. 2007. '*Inquiry into automatic number plate recognition technology'*, Issues paper 12. Parliamentary Travelsafe Committee, Legislative Assembly of Queensland.

UK Government 1998. "*Data protection Made Easy'*. At http://www.data-protection-act.co.uk/ accessed 7 July2008.

Wigan, MR & Clarke, RA. 2006, '*Social impacts of transport surveillance'*. Prometheus 4(24), 389-404.

Wigan, MR 2007, *Owning identity: one or many: do we have a choice?'*, In K Michael and MG Michael. '*From dataveillance to uberveillance and the realpolitik of the transparent society'*, Proc. 2nd RNSA Workshop on the Social Implications of National Security'. University of Wollongong. pp. 61-70.

Wigan, MR. 2008. "*Governance and Evidence Based Policy under a National Security Framework: If you cant contest who can you trust?*'. (this meeting)

Wood, DM [Ed.] '*A report on the surveillance society'*, for the Information Commissioner by the Surveillance Studies Network, London UK.

Acknowledgement:

The authors would like to thank Mr Murray Long of Murray Long & Associates for his detailed review comments.

14

Regulating the use of telecommunications location data by Australian law enforcement agencies

Rob Nicholls[1] and Michelle Rowland[2]

[1]Consultant, Gilbert + Tobin and PhD Candidate, School of Social Sciences and International Studies, University of New South Wales, [2]Lawyer, Gilbert + Tobin

Abstract

This paper sets out the regime for access to the “telecommunications data”, which includes location data and other metadata associated with communications in Australia under the amended Telecommunications (Interception and Access) Act 1979 (Cth). The paper examines this legislation which requires the delivery of location information to law enforcement agencies without defining “telecommunications data”. This raises the crucial question as to why Australia permits real time cell site level location information to be made available to law enforcement agencies on the authorisation of a public servant, rather than requiring approval of a judicial officer as is the case for call content warrants. This is in contrast with the US which require a court to find “probable cause”. At the very least, other jurisdictions require a judicial officer at the level of magistrate to be convinced that the agency needs the metadata on the balance of probabilities. In an environment where access to location data is more readily obtained by law enforcement agencies than in other countries, the paper also sets out the high level of compliance with the legislative intent.

Keywords: lawful interception, mobile telecommunication, location based services, hand over interface, assistance to law enforcement agencies.

1 Introduction

This paper takes a practical approach to the activities associated with lawful access to communications metadata and the interception of both telecommunications and stored communications under the current legislative regime. Lawful interception of voice communications has been practised for many years. However, changes in Australian legislation in 2007 have created a regulatory environment where there is increased access, without the need for a warrant, by law enforcement agencies to metadata associated with communications. This metadata is referred to as "telecommunications data" in the relevant legislation without there being a definition for the term. However, the relevant metadata includes the location of the target at the time of the communication. In 2007, there was amending legislation which permitted certain agencies to gain access to metadata associated with communications on a "near real time basis". The obligation is to supply telecommunications on a prospective basis to ASIO and law enforcement agencies. This paper discusses the implications that arise from the change in requirements for access to communications metadata and the practical implementation of such access.

We begin by considering some of the literature on interception of telecommunications and move on to look at the fundamental mechanisms involved in the handover of materials from a telecommunications carrier or carriage service provider to relevant law enforcement agencies using the European model (ETSI 2007). We then compare the current legislative framework and the drafting which must be interpreted by telecommunications carriers in Australia with the approach to law enforcement agency access to location metadata in each of the US and Europe. After this, the paper describes the practical implications of the legislative changes which have affected carriers and carriage service providers and the response made by those operators to demands (whether or not supported by warrants) imposed by law enforcement agencies. We then present an analysis of the issues that arise from these operator studies and draw conclusions.

2 Previous studies

The need for the appropriate and lawful interception of voice communications has been recognised for the past fifty years, if only because of the lawlessness of interception in the first half of the twentieth century (Branch 2003). In Australia, the focus from 1960 to 2005 was only on regulating the interception of voice. There were some doubts about the legality of access to stored communications (for example, emails) and agencies obtained data either by a search warrant or an interception warrant (Holland 2004). However, the increasing options for communications and the potential for criminals to use communications mechanisms such as instant messaging (Nolin 2006) and the lack of security of this technology (Williams and Ly 2004) has led to a change in the Australian legislation. These amendments created a difference in the regulatory approach to live communications compared with stored communications (Bronitt and Stellios 2006; Nicholls and Rowland 2007).

Australia is not alone in changing the legislative and regulatory environments to attempt to address new technologies. South Africa took a simple approach and described communications as either "direct" or "indirect" and provided an interception regime for both (Bawa 2006). In the USA, there was debate about the more prescriptive and proscriptive approaches in the amendments to the *Communications Assistance for Law Enforcement Act* (US) (**CALEA**) which now encompasses internet-based communications environments and services (Schwaderer 2007). The debate included input from some of the original architects of the internet (Landau 2005; Bellovin, Blaze et al. 2006). Although this debate argued that there were technical as well as social risks to amending CALEA, the technical standards for emerging technologies already provided lawful interception access ports (Miettinen 1999; Milanovic, Srbljic et al. 2003; Milanovic, Srbljic et al. 2003; Street 2003; Fonknechten, Ghribi et al. 2004; Open Mobile Alliance 2005; Gidari 2006; Gratzer, Naccache et al. 2006; ETSI 2007).

Much of the focus of the debate over interception capability has been in respect ofVoice over Internet Protocol (**VoIP**) (Drinan, Fontaine et al. 2005; Miller, Levine et al. 2005; Del Bianco 2006). Whereas the amendment to CALEA to introduce an obligation for interception ofVoIP services was a new obligation, this is not the case in Australia.

The *Telecommunications (Interception and Access) Act* 1979 imposes an obligation on all carriage service providers with facilities in Australia to maintain an interception capability (in section 191) and to provide assistance to relevant agencies (in Part 4). There was also another significant effect from the legislative amendments in that the obligations on carriers and carriage service providers were moved from the *Telecommunications Act* 1997 (Cth) to the *Telecommunications (Interception and Access) Act* 1979. The prohibitions on disclosure of communications and communications metadata remain in sections 276-278 of the *Telecommunications Act* 1997 but the *Telecommunications (Interception and Access) Act* 1979 sets out circumstances where these prohibitions no longer apply (as summarised in section 171). There remains in Part 14 of the *Telecommunications Act* 1997 an obligation on carriers and carriage service provider to give authorities such help as is reasonably necessary for the purposes of (among other things) enforcing the criminal law.

3 The European model

The European Telecommunications Standards Institute (**ETSI**) has developed a model for the interaction between law enforcement agencies and carriers or carriage service providers. There are three broad interfaces between telecommunications operators and law enforcement agencies and these are set out in (ETSI 2007).

As described by the authors previously (Nicholls and Rowland 2007), service provider interfaces with the law enforcement agency (**LEA**) on three levels. The first level, referred to as handover interface 1, is simply the administrative arrangements between the LEA and the service provider and is an ongoing relationship. In Australia, this may be a service agreement and service level agreement with the relevant LEAs. In other countries, this administrative interface is far more standardised and has, as a result, a higher level of transparency. The second level, referred to as handover interface 2, is the mechanism by which the service provider delivers communications metadata but not the content of communications. Typically, in Australia, this information is provided as part of the carriage service provider's "reasonable assistance" obligations under the *Telecommunications Act* 1997 set out above. This type of information would include, in respect of an identified individual, the addresses or phone numbers of communications to and from that individual, information as to the time of the communication and limited information as to its nature (for example, the duration of a voice call or the size of an email). The final level, referred to as handover interface 3, is the mechanism by which the service provider delivers communications content to the LEA. In Australia, this material is delivered in response to a warrant.

This model provides a useful means to consider the development of interception and access over time. The model is general enough to be applicable to both voice and non-voice communications. It is also able to distinguish between communications metadata and the content of those communications.

4 Australia, Europe and the USA

The 2007 amendments to the *Telecommunications (Interception and Access) Act* 1979 change the nature of the delivery of communications metadata. Until the introduction of the amendments, communications metadata was supplied by carriers on a historical basis. That is, "call associated data" in Australia and "interception related information" in Europe (also generically known as metadata) was supplied after the calls were made by the target. The amendments introduced a new (and undefined) term for this metadata of "telecommunications data". In response to a request by a law enforcement agency, a carrier is obliged to provide metadata on a "prospective" basis. This metadata is to be supplied to the agency on a "near real time" basis thereby allowing live tracking of target movements and associations.

The relevant agency must certify the need for prospective data and the legislation provides that the certification must be at a senior level as well as in respect of a crime for which the maximum penalty is imprisonment for three years. The certifying bureaucrat must also have regard to how much the privacy of any person or persons would be likely to be interfered with. However, the right to certify can be delegated within the agency. There is no requirement to have the need tested by obtaining a warrant from a member of the Administrative Appeals Tribunal, which is the position which applies to the other forms of surveillance authorised under the *Telecommunications (Interception and Access) Act* 1979 (Bronitt and Stellios 2006). The range of agencies which can seek telecommunications data on a prospective basis is large and includes ASIO, the State and Federal police, customs and the state based crime commissions.

This section demonstrates that the supply of information on a historical basis in response to a law enforcement agency request for assistance has been common but that the supply of prospective data, and particularly real time location information, is unusual. In TV police shows such as "Law and Order", there is often a call to "pull the LUDs" (local usage details)– in other words, to obtain, without a warrant, historical call records. However, the same characters often have a bigger problem with showing "probable cause" which is the US test required for location based information, even at cell site level.

In the US, there are three conceptual ways in which communications content and communications metadata can be obtained by law enforcement agencies (Gleave 2007). The first is the delivery of historical call information or local usage details. This is the outgoing historical record which can be obtained by subpoena from the local telephone company or mobile operator provided that the telephone number and identity of the target can be offered. Prepaid mobile services or "disposable phones" do not have an individual identified with them (and this is also the case in the UK). The second form of access is a "pen register" authority. This provides details of the use of a telephone service (sent and received calls) on a prospective basis (excluding the delivery of communications content) and requires a warrant from a judge at the magistrate level. The test for this warrant is certification by a law enforcement office that "the information likely to be obtained is relevant to an ongoing criminal investigation" (Phillips 2003). The final level is for the content of communications and this requires a "tap and trace" warrant from a more senior judge who has to be persuaded that there is "probable cause" (McLaughlin 2007). This test is stronger than an assertion by a law enforcement office that the warrant is reasonably necessary. The Oxford Dictionary of American Law defines it as "information sufficient to warrant a prudent person's belief that the wanted individual had committed a crime (for an arrest warrant) or that evidence of a crime or contraband would be found". This is higher than the more commonly applied standard in the criminal law of belief or suspicion based on reasonable grounds.

The obligations imposed on operators are given under CALEA. In addition, there are other requirements to provide information under the Patriot Act. Access to location based information under CALEA has always been contentious. The initial expectation was that location based information would be supplied in response to a pen register authority. However, the Federal Communications Commission (**FCC**) limited such location information to cell site identification with regard to wireless communications, "drawing an analogy to street address information already available to law enforcement for wireline telephone numbers" (Nylund 2000, p330). Further, there has been specific clarity that GPS functionality in handsets is not included in the CALEA obligations (Richmond 2007) although it is under the Patriot Act (Karim 2004).

That is, the delivery of location based information is only permitted in response to a magistrate's warrant under CALEA. Even critical comment on the FCC interpretation of CALEA has the assumption of a warrant to collect location information (Case Note 2004; Dirvianskis 2007). Ian Samuel argues that a magistrate's warrant is not sufficient even for historical location based information and that probable cause is constitutionally required (Samuel 2008). Importantly, he argues for transparency in the debate about the evolution of warrant powers:

> A robust public debate about location privacy is essential for good policy. That discussion should not occur without reference to shared Constitutional norms about search; and in the reading of statutes, Congress should not be presumed ignorant of them.

Other work suggests that Samuel should also have considered that even a warrant may be insufficient. Steven B. Toeniskoetter argues "the Fourth Amendment is also likely to impose restrictions on how and when law enforcement may acquire prospective cell site data" (Toeniskoetter 2007). However, the Patriot Act does provide alternatives for a lower threshold of proof (Shields 2002). Both Shields and Charlotte Twight share the fear that location based service information, among other things, will turn mobile use into a panopticon for law enforcement agencies (Twight 2001) and Laurie Lee argues that the lack of clarity on the issue requires a new legislative approach (Lee 2003).

The European Union requirements are similar to those set out in CALEA, although individual country's implementations may have a significantly lower degree of flexibility as the US legislation (Koops and Bekkers 2007). These were incorporated into the *Regulation of Investigatory Powers Act* 2000 (UK) (**RIPA**) which provides for a similar delivery of location based information in response to a warrant as CALEA (Yeates 2003). RIPA has a concept of "communications data" similar to the Australian legislation. However, RIPA defines the meaning of the term and there are also publicly available guidelines to assist carriers in understanding the requirements (Sutter 2001). The French legislation also requires a court order for location based information on a prospective basis (Gorge 2007) and the court is particularly strict in its requirements for the wording of warrants (Gratzer, Naccache et al. 2006).

The value of location information to law enforcement agencies, even if it is only at the level of cell site, is not contested (Clark 2006). Further, there has been some indication from DoCoMo that some industry participants do not have a clear understanding as to the privacy issues (Ackerman, Kempf et al. 2003).

In summary, despite the debates that have occurred as to which court should authorise the disclosure of prospective data, both the USA and European Union member states have regulatory environments for the deliver of communications, content and communications metadata to law enforcement agencies, which require a court to decide the merits of assertions as to need presented by law enforcement officers. Judicial involvement in the telecommunications interception is constrained by constitutional law, which means that judicial officers are only reviewing warrants in a personal rather than judicial capacity. This has meant that federal judges, though eligible to authorise warrants under the *Telecommunications (Interception and Access) Act* 1979, have largely withdrawn from this role, and Administrative Appeal Tribunal members have taken over (Bronitt and Stellios 2006). That is, the absence of any judicial involvement in the authorisation process of metadata is consistent with a general trend and the preference for security over privacy exhibited by consecutive Australian governments (Bronitt and Stellios 2006). Even with the need for warrants, the Australian regime is significantly more intrusive than that in the US with "an Australian telephone being 23 times more likely to be intercepted than an American telephone" (Rowland and Alderson 2008). This comparison does not include US data on 'consensual taps' where one party to the communication (typically, an undercover police officer or informer) agrees to the interception. In such cases, there is no requirement to obtain a warrant in the US. Equivalent conduct clearly requires a warrant in Australia (whether one party consented or not).

5 Implementation by carriers and carriage service providers

As a practical matter, mobile operators in Australia have the capacity to deliver call associated data on a prospective basis. This means that the effect of the 2007 legislative amendments is simply a mechanism to require operators to deliver the communications metadata. However, this does not mean that law enforcement agencies are able to locate targets with any great precision. Location based services use multiple techniques in order to determine the location of a customer and the legislative package does not, making a reasonable assumption about the nature of "telecommunications data", impose an obligation on carriers to provide a location based service. Rather, it requires that cell site information is provided.

Carriers typically provide more accurate location based information in response to particular safety of life situations. When there is a potential suicide, for example, a carrier may assist authorities by triangulating the position of a person based on a handset in operation. This is not a standard location based service and requires significant engineering effort. Further, it is not the type of information that would lend itself to prospective data delivery.

The increasing used of location based services (Bowen and Martin 2007) means that there should be no assumption that the location based information associated with such services would not fall into the definition of "telecommunications data" at some point in the future. The major reason for the absence of a definition of telecommunications data in the legislation is that the term was expected to evolve with technology over time. In particular, the development of standards for the presentation of location information (Adams, Ashwell et al. 2003) potentially herald this. In turn, this leads to the biggest issue arising from the regulatory changes which faces mobile operators in Australia. As has been pointed out in the past, mobile operators have been more than willing to ensure that they comply with their obligations in meeting the legislative regime and in many cases deliver more than is required under the poorly drafted legislation which imposes broad duties of assistance (Nicholls and Rowland 2007). The likelihood is that the criminal enforcement agencies and ASIO will decide that telecommunications data has a larger meaning than merely call associated data. As this changes over time, there is no provision for a review of the undefined term.

The problem is compounded by the fact that law enforcement agencies represent an epistemic community. That is, the agencies discuss issues with each other and created a consensus view which relates to all of the agencies' needs. As a result, the meaning of terms such as "telecommunications data" will evolve more rapidly than would be determined by any one of the agencies. In effect, the legislative framework under the *Telecommunications (Interception and Access) Act* 1979 provides an environment where the metadata delivered is determined by the agencies which require the data at their sole discretion. Whereas there is typically agency design in the way that communications content and metadata is delivered (Nylund 2000), the absence of external review, even on a cursory basis, does not represent regulatory best practice. Indeed, as the legislation gives the Attorney-General the power to determine the method of deliver of communications content consistent with international standards (section 189), it is odd that the delivery of communications metadata is left entirely in the hands of the agencies.

To some extent, there is already evidence of this in the delivery of communications content. The 2008 amendments to the *Telecommunications (Interception and Access) Act* 1979 have significant effect (Rowland and Alderson 2008):

> The proposed amendments mean that a named person warrant, issued in respect of devices, will authorise interception of communications on *any* telecommunications device that the person *uses*, or *is likely to use* to the extent that they are known at the time of applying for the warrant. ASIO and other law enforcement officers would be able to intercept all communications made by means of any telecommunications device used by a named person of interest, rather than first identifying in the warrant all of the particular telecommunication devices to be intercepted.

The legislative changes are also generally more profound than simply changing the obligations for supply of communications metadata. All of the obligations associated with the provision of communications content and communications metadata have been moved from the *Telecommunications Act* 1997 to the *Telecommunications (Interception and Access) Act* 1979. The effect of this change is to remove (except by limited and partial reference) all of the objects of the *Telecommunications Act* 1997. This changes the regulatory paradigm for interactions between carriers and law enforcement agencies from one based on self-regulation and increasing diversity of services to one where the legislation has no stated objects. There is also a significant widening of the scope of the legislation. The previous regime imposed an obligation for interception and assistance on carriers and carriage service providers with distinctions between the two. The *Telecommunications (Interception and Access) Act* 1979 does not draw such a distinction and, indeed, conflates the two concepts into the single defined term "carrier" in section 5.

6 Conclusions

The Australian legislation grants power to law enforcement agencies to obtain location based communications metadata on a prospective basis without the need for a warrant or other external oversight (for example, authorisation by a member of the Administrative Appeals Tribunal). This power is unusual when compared with either the US or European countries. Given that the balance between the needs of law enforcement agencies and others has been in favour of the law enforcement agencies for some time (Bronitt and Stellios 2005; 2006), the recent changes to the regulatory regime for interception and access are surprising both in the extent of powers provided to agencies and the lack of transparency in the exercise of those powers. Perhaps the lament of Bronitt and Stellios is worth repeating (Bronitt and Stellios 2005, p887):

> In Australia, the lack of a Bill of Rights informing legislative design at federal and state level has meant that law enforcement interests have tended to prevail over these other interests.

We have shown that the debate about warrants for location based information in the US has focused on which court (rather than whether a court) should be applied to for location metadata. In Europe a warrant was assumed and the doubts expressed by carriers in relation to the meaning of the term associated with metadata has been addressed by a code of practice. As a result, Australia appears to be isolated in its approach of placing the power to have location metadata supplied on a prospective basis to law enforcement agencies.

Given that the use of warrants is already extensive in Australia, perhaps it is time to review whether the legislative framework and the associated regulatory regime represent the appropriate balance between the needs of law enforcement agencies and citizens. After all, the probable cause test is not so onerous that it could not be applied in Australia and members of the Administrative Appeals Tribunal will likely be just as available to the relevant agencies as they are for the existing warrant regime.

References

Ackerman, L., J. Kempf, et al. (2003). Wireless Location Privacy: A Report on Law and Policy in the United States, the European Union, and Japan. San Jose, NTT DoCoMo.

Adams, P. M., W. Ashwell, et al. (2003). «Location-based services — an overview of the standards.» *BT Technology Journal* 21(1): 34-43.

Bawa, N. (2006). The Regulation of the Interception of Communications and Provision of Communication Related Information Act. *Telecommunications Law in South Africa*. L. Thornton, Y. Carrim, P. Mtshaulana and P. Reyburn. Johannesburg, STE Publishers.

Bellovin, S., M. Blaze, et al. (2006). Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. Washington, Information Technology Association of America.

Bowen, C. L. and T. L. Martin (2007). A Survey of Location Privacy and an Approach for Solitary Users. *40th Annual Hawaii International Conference on System Sciences*. Hawaii, IEEE.

Branch, P. A. (2003). Lawful Interception of the Internet. Melbourne, Centre for Advanced Internet Architectures, Swinburne University of Technology.

Bronitt, S. and J. Stellios (2005). "Telecommunications interception in Australia: Recent trends and regulatory prospects." *Telecommunications Policy* 29: 875-888.

Bronitt, S. and J. Stellios (2006). "Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?" *Prometheus* 24(4): 413-428.

Case Note (2004). "Who Knows Where You've Been? Privacy Concerns Regarding the use of Cellular Phones as Personal Locators." *Harvard Journal of Law & Technology* 18: 307-317.

Clark, M. W. (2006). "Cell Phone Technology and Physical Surveillance." *FBI Law Enforcement Bulletin* 75(5): 25-32.

Del Bianco, M. C. (2006). "Voices Past: The Present and Future of VoIP Regulation." *CommLaw Conspectus* 14: 365-401.

Dirvianskis, S. E. (2007). "American Council on Education v. FCC: Proper Outcome, Lack of Clarity in the Interpretation of CALEA." *Jurimetrics* 47: 463-477.

Drinan, H., N. Fontaine, et al. (2005). «News Briefs.» *Security & Privacy Magazine, IEEE* 3(6): 7-8.

ETSI (2007). Lawful Interception (LI): Handover interface for the lawful interception of telecommunications traffic. ETSI ES 201 671 V3.1.1 (2007-05). Sophia Antipolis Cedex - FRANCE, European Telecommunications Standard Institute.

Fonknechten, D., B. Ghribi, et al. (2004). «Service Aware Intelligent GGSN.» *Alcatel Telecommunications Review* 1st Quarter 2004: 2-10.

Gidari, A. (2006). "Designing the Right Wiretap Solution: Setting Standards under CALEA." IEEE Security and Privacy (May/June 2006): 29-36.

Gleave, S. (2007). "The mechanics of lawful interception." *Network Security* May 2007: 8-11.

Gorge, M. (2007). "Lawful interception – key concepts, actors, trends and best practice considerations." *Computer Fraud & Security*(September 2007).

Gratzer, V., D. Naccache, et al. (2006). Law Enforcement, Forensics and Mobile Communications. *4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, IEEE**:** 256.

Gratzer,V., D. Naccache, et al. (2006). *Law enforcement, forensics and mobile communications*. Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on.

Holland, B. (2004). "Overtaking privacy in the telecommunications transit lane." *Privacy Law and Policy Reporter* 10.

Karim, W. (2004). "The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring." *Journal of Law & Policy* 14: 485-515.

Koops, B.-J. and R. Bekkers (2007). "Interceptability of telecommunications: Is US and Dutch law prepared for the future?" *Telecommunications Policy* 31: 45-67.

Landau, S. (2005). "Security, Wiretapping and the Internet." *Security and Privacy Magazine, IEEE* (December 2005): 26-33.

Lee, L. T. (2003). "Can police track your wireless calls? Call location information and privacy law." *Cardozo Arts & Entertainment Law Journal* 21(2/3): 381-406.

McLaughlin, K. (2007). "The Fourth Amendment and Cell Phone Location Tracking: Where Are We?" *Hastings Communications and Entertainment Law Journal* 29: 421-446.

Miettinen, K. (1999). Lawful Interception in GPRS/UMTS Network. Helsinki, University of Helsinki.

Milanovic, A., S. Srbljic, et al. (2003). *Methods for lawful interception in IP telephony networks based on H.323*. EUROCON 2003. Computer as a Tool. The IEEE Region 8.

Milanovic, A., S. Srbljic, et al. (2003). *Distributed system for lawful interception in VoIP networks*. EUROCON 2003. Computer as a Tool. The IEEE Region 8.

Miller, H. G., H. D. Levine, et al. (2005). "Welcome to convergence: surviving the next platform change [Internet protocol]." *IT Professional* 7(3): 18-25.

Nicholls, R. and M. Rowland (2007). Message in a bottle: Stored communications interception as practised in Australia. *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society: The Second Workshop on the Social Implications of National Security*. M. Michael and K. Michael. Wollongong, Wollongong University.

Nolin, C. A. (2006). "Telecommunications as a Weapon in the War of Modern Organized Crime." *CommLaw Conspectus* 15(Fall 2006): 231.

Nylund, J. J. (2000). "Fire With Fire: How the FBI Set Technical Standards for the Telecommunications Industry under CALEA." *Commlaw Conspectus* 8: 329-348.

Open Mobile Alliance (2005). Push to talk over Cellular (PoC) - Architecture. La Jolla, Open Mobile Alliance.

Phillips, D. J. (2003). "Beyond Privacy: Confronting Locational Surveillance in Wireless Communications." *Communications Law and Policy* 8(1): 1-24.

Richmond, D. P. (2007). "Can you find me now?—Tracking the Limits on Government Access to Cellular GPS Location Data " *CommLaw Conspectus* 16: 283-319.

Rowland, M. and S. Alderson (2008). "New telecommunications interception and access proposals: the first or last of many?" *Communications Law and Policy Bulletin* (May 2008).

Samuel, I. (2008). "Warrantless Location Tracking." *NYU Law Review* 83.

Schwaderer, C. (2007). Lawful surveillance systems: Enforcing justice while protecting individual privacy. *CompactPCI and AdvancedTCA Systems*.

Shields, P. (2002). Technology Determinism, the State and Telecom Surveillance. *Networking Knowledge for Information Societies: Institutions & Intervention*. R. Mansell, R. Samarajiva and A. Mahan. Delft, Delft University Press.

Street, M. D. (2003). *Interoperability and international operation: an introduction to end to end mobile security*. Secure GSM and Beyond: End to End Security for Mobile Communications, IEE Seminar on (Digest No. 2003/10059).

Sutter, G. (2001). A Tale of Two Interception Regimes: RIP v CALEA, a comparison. *16th BILETA Annual Conference*. Endinburgh, BILETA.

Toeniskoetter, S. B. (2007). "Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data." *Richmond Journal of Law and Technology* 13(4): 16-65.

Twight, C. (2001). "Conning Congress: Privacy and the 1994 Communications Assistance for Law Enforcement Act." *The Independent Review* 6(2): 185–216.

Williams, N. and J. Ly (2004). Securing Public Instant Messaging (IM) At Work. Melbourne, Centre for Advanced Internet Architectures, Swinburne University of Technology.

Yeates, J. (2003). "CALEA and the RIPA: THE U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World." *ALB. L.J. SCI. & TECH.* 12: 125-166.

15

User acceptance of location-based services for emergency management in Australia

Anas Aloudat

PhD Candidate, School of Information Systems and Technology, University of Wollongong

Abstract

Over the past few years, governments and mobile service providers have started to exploit location-based services (LBS) and their underlying technologies for the purpose of emergency management (EM). LBS emerged as a practical solution for determining a user's location, facilitating the delivery of services based on the derived position information. The value of these services can be seen especially in the coordination of emergency management procedures. Nonetheless, the utilisation of LBS in emergency management is not yet widespread in Australia. As a result, this study investigates the introduction of LBS as part of a holistic approach for managing emergencies and hazardous situations. As the solution relies on an individual's willingness to use the services, the study will examine the users' acceptance of LBS and the potential consequences from the realisation of these solutions.

Keywords: location-based services, emergency management, hazards, user acceptance

1 Introduction

LBS are electronic services that take into account the geographic area of a mobile phone, and provide the mobile phone user with services based on his/her location information (Küpper, 2005). The applicatory possibilities of LBS solutions make them well worth exploring in the domain of EM since users' location(s) can be determined by using available positioning techniques, which then facilitates the provision of pertinent services based on the derived location information. For example, with LBS in use, the mobile service provider in cooperation with government agencies will be able to send relevant alerts and information regarding major incidents or events such as a severe weather warning or a terrorist attack or natural disaster, if it happened in the vicinity of the mobile phone user(s). Another example would be to find the almost precise geographical location of a mobile user in the case of a 000 emergency call.

2 Background

Several governments have started to utilise LBS applications in EM. For example, in the United States, the Federal Communications Commission (FCC) has advanced the use of LBS as part of the traditional 911 emergency calls system, which resulted in the introduction of the Enhanced 911 (E911). A similar system under the name of (E112) has also been initiated in the European Union. In these systems, the mobile companies are required to report the location information of an originated emergency call to an emergency dispatch centre within accuracies between 50 to 150 metres of the caller (International Telecommunication Union, 2002).

Several researchers have already investigated the use of different mobile technologies and services, including LBS, as practical solutions to deliver alerts, notifications, and emergency information to users (Krishnamurthy, 2002; Weiss et al., 2006; Aloudat et al., 2007). However, scarcely few studies have undertaken the task of investigating the consequences of utilising LBS in EM. In particular, the concerns and issues the general user might have regarding the introduction of these services as part of a feasible solution in the emergency management domain. To the best of the researchers' knowledge, no formal studies have examined user acceptance of LBS for emergency management in Australia. This researcher believes that there is a pressing need to explore the potential drivers of acceptance in order to provide a suitable modus to understand individual's beliefs about such consequences. As a result, this study contests that an early understanding of the theory-based literature about acceptance is of paramount importance as it will determine the underlying motivations that would influence individuals' perceptions regarding the use of LBS in EM.

What follows is a discussion of the meaning of "acceptance" in Information Systems and Technology (IST) research. An overview of the conceptual development of the research model proposed and a summary of its constructs. Furthermore, a brief description of the methods that will be used to collect the research data is also presented.

3 The notion of acceptance

Understanding why some people accept a technology while others do not has been one of the most challenging issues in IST research (Swanson, 1988). A central discipline emerged which attempts to understand the factors that may predict individual acceptance or rejection.

The Oxford English Dictionary (2002) defines acceptance as:

> "The act or fact of accepting, or taking what is offered, whether as a pleasure, a satisfaction of claim, or a duty". It also defined it as "of things: favourable consideration, approval; and hence, of statements, theories, etc".

It can be deduced from the definition that acceptance is related to satisfaction. This is perhaps the reason why several IST acceptance studies have treated the two concepts equivalently (Cho & Agrusa, 2006; Saadé & Kira, 2006). Other studies viewed satisfaction as a surrogate measurement of acceptance and IST success (Ives et al., 1983; Al-Gahtani & King, 1999; DeLone & McLean, 2002). However, acceptance itself, has not been widely presented as a solitary surrogate of IST success (Despont-Gros et al., 2005) since it might not be possible to determine success by acceptance alone. Nonetheless, it has been recognised as one of the most pivotal factors that could predict the successful adoption and usage rates of new information systems and technologies (Swanson, 1988; Davis, 1989,1993; Al-Gahtani, 2002).

The perspective of technology acceptance has been described by Dillon and Morris (1996) as the "demonstrable willingness within a user group to employ information technology for the tasks it is designed to support". Although user acceptance has been investigated here from an organisational level, Dillon and Morris conceived the individual's willingness to use as the initial phase of acceptance. The definition also implies the intentional and prospective use of the technology. This substantiates what Dillon (2001) has argued that acceptance theories are more concerned with individuals' prepense decisions to use rather than their non-discretionary and unintentional use of the technology.

Swanson (1988) also related acceptance with the willingness to use as he interpreted acceptance as "potential user's predisposition towards personally using a specific system". Such tendency has been recognised to be moulded in two interrelated stages (Kalish, 1985; Weenig & Midden, 1991; Bulte & Lilien, 2001). The first is awareness, where the individual learns about the existence of a technology and then gains some understanding about it. The second is evaluation, where the individual forms some kind of assessment based on the obtained knowledge about that technology (Bulte & Lilien, 2001). Eventually, the assessment leads into the decision of accepting or rejecting the technology.

Measuring acceptance in technology-driven contexts, nonetheless, is difficult as the construct is a subjective sentiment that is appraised differently by different users (Lee et al., 1995). In addition, the construct itself holds a verity of meanings in the literature (Karahanna, 1999; Rawstorne, 2005). Accordingly, researchers' endeavours to operationalise a verifiable construct, to be defined from a quantitative point of view, have resulted in the formation of several acceptance theories and models (Agarwal, 2000). As a result, literature has witnessed a plenitude of acceptance studies in the past two decades as the existence of several theoretical models have advanced researchers with the needed base for understanding and predicting acceptance, usage, and adoption behaviours (Malhotra & Galletta, 1999; Rawstorne, 2005). In line with prior studies, and building upon well-known technology acceptance theories and models, the following section presents an overview of the research approach and provides a summary of the research constructs that will be employed to predict user acceptance of LBS.

4 Conceptual development: An overview

4.1 Assurance of control mechanisms

Since a user's location can be determined by using different a variety of positioning techniques (Küpper, 2005), the need arises for creating safeguards to protect individuals and assure their control over personal information (Morris, 2002). However, Michael et al.(2006) discerned that even developed countries like the United States and Australia do not have yet special legislations that can handle disputes and issues that originate from the utilisation of LBS. Given this predicament, it could be argued that one of the main impediments of LBS acceptance would be users' perception of the lack of dedicated mechanisms that could protect and safeguard their personal location information.

Xu and Teo (2004) have proposed three control mechanisms in order to alleviate users' concerns. They are technology self-based, institution-based via self-regulations, and institution-based via government legislation. The main proposition here is that if users have higher perceptions of control over their personal location information, then it would positively influence their intentions to use LBS (Xu & Teo, 2005). Technology self-based assurance of control refers to the ability of an individual to exercise a direct control over his/her personal information via the technical features of the LBS device. For example, a user can determine when to opt out of a particular LBS or define the preferred accuracy level to which service providers are allowed to track his/her device.

When the technology is neither ready nor supported, the user might consider other alternatives of control assurance. One option is the institution-based via self-regulations, in which the industry exercises a set of policies to assure the privacy of individuals' location information and LBS transactions (Xu & Teo, 2004). The relationship between users and service providers are governed through a set of stipulated obligations and established codes and principles within the industry itself. A close example is "the code of good practice for the provision of mobile services in the UK". The code regulates the relationship between users and the industry and complies with applicable law in the case of rising disputes and conflicts (Code of Practice of Passive Location Services in the UK, 2006).

Another possible alternative is institution-based via legislation. In this case, relevant government policies and explicit laws and regulations would exist within the legal system to ensure the proper disclosure and use of personal location information (Xu & Teo, 2004). The assurance of government legislations might provide the maximum safeguards for protecting users' privacy as illegal behaviours are deterred through the legal system in use. Power forces (i.e. government agencies) would act as control agents on behalf of the users to exercise proxy control over their location information (Xu & Teo, 2004,2005).

While some researchers emphasise that the maximum success of safeguards would be achieved if they were to become a component in the technology itself (Morris, 2002), the technology might not be always ready, available or favoured. Therefore, perlustrating distinctive forms of control assurance mechanisms would provide credible evidence and reasonable futuristic insight apropos of utilising any of these mechanisms within LBS solutions. Zweig and Webster (2002) argued that individuals will accept the new technology, if they perceive more control over their information. What matters here is how users perceive the most dependable method(s) that are capable of protecting their location information, thus alleviating any concerns they might have towards accepting LBS and its related technologies.

The practical investigation of assurance of control mechanisms stems from the fact that numerous studies have identified privacy concerns as one of the main impediments of using information technology systems including LBS (Esrock & Ferre, 1999; Hoffman et al., 1999; Hann et al., 2002; Ho & Kwok, 2003; Bauer et al., 2005; Junglas & Spitzmuller, 2005; Parasuraman et al., 2005; Scharl et al., 2005; Xu et al., 2005; Michael & Salter, 2006; Michael et al., 2006). It is noted, nonetheless, that *assurance of control* has been scantly investigated in acceptance research. Furthermore, almost no study has examined the relationship between control mechanisms and user acceptance of LBS. As a result, key informant's opinions regarding *assurance of control* will be investigated as part of this research. Assurance of control is expected to impact positively on users trust towards the use of LBS.

4.2 An Acceptance Model of Location-Based Services

A literature review has been conducted to explore, identify, analyse, and critically assess the factors that would likely influence individuals' beliefs regarding the use of LBS. These factors, summarised in Table 1, which either encourage or hinder acceptance have been discussed in the light of previous studies on different wireless mobile technologies including LBS. It could be argued, nonetheless, that the factors should be based on beliefs that are directly elicited from potential users and not predetermined by the research. However, the method has been completely justified by Taylor and Todd (1995) and Venkatesh and Brown (2001) on the basis that there is a wealth of existing research on information systems and technology acceptance, which minimises the need to extract beliefs anew for each new acceptance setting.

Table 1 Summary of the factors and their definitions

Factor	Description of the adopted working definition	Based upon
Individual's attitude towards the use of LBS	Individual's positive or negative feelings towards using LBS in emergencies.	Fishbein & Ajzen (1975)
Individual's intention to use LBS	Individual's decision to engage or not to engage in using LBS in emergencies.	Fishbein & Ajzen (1975)
Trust	Willingness of the potential LBS user to be vulnerable to the outcome of LBS based on the expectation that the services will perform particular actions important to the trustor, irrespective of the ability to monitor or control the LBS service provider.	Mayer et al.(1995), Junglas & Spitzmuller (2005)
Risk as perceived by the potential user	LBS user belief that there is some probability of suffering a loss in using LBS for emergencies.	Pavlou & Gefen (2004)
Perceived usefulness	Individual perception that using LBS for managing emergencies will be useful to him/her.	Davis et al.(1989)
Perceived ease of use	The degree to which the prospective user expects LBS to be free of effort.	Davis et al.(1989)
Visibility	The extent to which individual see LBS are being used.	Agarwal & Prasad (1997)
Perceived service qualities	A global judgment, or attitude, relating to the superiority of the service.	Parasuraman et al.(1988)
Perceived currency	Individual's perception of receiving up-to-date service information	Zeithaml et al.(2000), Yang et al.(2003)
Perceived accuracy	Conformity of LBS with its perceived attributes.	Zeithaml et al.(2000), Yang et al.(2003)
Perceived responsiveness	Individual's perception of receiving a prompt LBS service.	Parasuraman et al.(1988), Liljander et al.(2002),Yang et al.(2003)

The factors are integrated into a research model that extends and builds upon the Theory of Reasoned Action (TRA) as applied to a technology-specific perspective in the form of the Technology Acceptance Model (TAM). See Figure 1. TAM is a special adaptation of TRA. It has been introduced by Davis (1986; 1989) in order to

> "provide an explanation of the determinants of computer acceptance that is general, capable of explaining user behaviour across a broad range of end-user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified" (Davis et al., 1989).

The model postulates that the usage or adoption behaviour is predicted by individual's intention to use the new IST. Behavioural intention is determined by individual's attitude towards the use of the new IST. Attitude, in turn, is influenced by two key beliefs: perceived ease of use; the individual's perception concerning the amount of effort required to use the new IST, and perceived usefulness; individual's perception concerning the degree to which using the technology will improve performance. The model grants a basis for investigating the influence of external factors on its internal beliefs, attitudes, and intentions (Davis et al., 1989).

Extending TAM with the aforementioned factors is expected to yield an improvement to the model's ability to predict LBS acceptance, while providing a justifiable theoretical approach for integrating the new variables within the nomological structure of TRA. A highly validated approach that has been exploited before by Pavlou (2003) for studying consumer acceptance of electronic commerce.

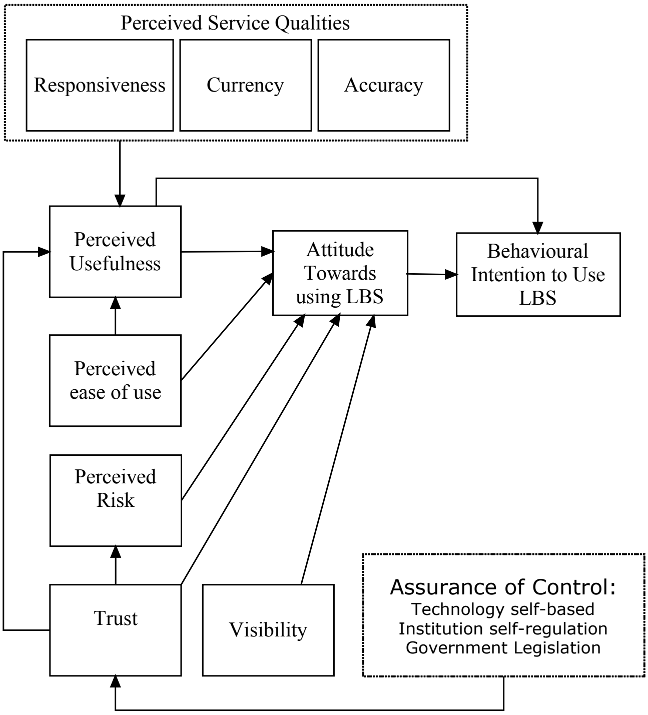


Figure 1: User Acceptance of LBS Research Model

4.3 Methods of data collection

The research model incorporates the constructs that are considered to be the most relevant to LBS distinct characteristics. The same variables also constitute the basic structure of the main research instrument i.e. the survey. The survey itself comprises three sections. The first section is a simple introduction about LBS. It is intended to give the participant a principal understanding about the possible use of LBS applications in emergencies and hazardous situations.

The second section presents the research vignettes. Vignettes are "brief stories or scenarios that describe hypothetical characters or situations to which a respondent is asked to react" (Martin, 2004). The written word is the common form of a vignette, although it can be presented in a variety of other forms such as video, pictures, or cartoon animation (Wilks, 2004). Presser et al. (2004) and Martin (2004) discerned that the use of scenarios and vignettes appears well-suited when there is a need to:

i Explore how people think about a conceptual domain
ii Test whether respondents' interpretations of concepts are consistent with those that are intended
iii Analyse the dimensionality of survey concepts
iv Diagnose question-wording problems and assess uniformity of meaning.

As vignette's depict hypothetical situations that are beyond the idiosyncrasies of the respondent's life, they offer a less personally threatening way to stimulate judgments and explore sensitive issues like emergencies (Finch, 1987; Schoenberg & Ravdal, 2000). Through the use of vignettes, participants are encouraged to project how they think they or other people would react in a given situation. With such indirect forms of questioning, respondents are expected to provide their real responses as they will not perceive that they are personally evinced in the given situation, rather, the person that is depicted in the given vignette (Fisher, 1993; Parboteeah, 2005). As a result, vignettes are expected to reduce the likelihood of social desirability effects (Havlena & Holbrook, 1986; Fisher, 1993), which is the situation where respondents reply in a way that they think is more socially appropriate (Cook & Campbell, 1979). Consequently, vignettes are expected to elicit accurate responses while, at the same time, involve respondents in creating a meaning regarding LBS and their potential use in emergencies (Schoenberg & Ravdal, 2000).

By using vignettes to define the meaning of LBS amongst a large number of participants, the approach will provide the efficiency of quantitative data with a wealth of information that is closer to qualitative research (Finch, 1987). However, similar to any other research method, vignettes have disadvantages as well. For example, the use of hypothetical situations might be criticised for not being realistic. Nonetheless, their merit as a research method has been well-documented (Finch, 1987; Martin, 2004; Morrison et al., 2004; Presser et al., 2004). Further, their use could maximise precision by allowing the investigator to operationalise some of the research constructs, something that may not be possible under the available circumstances (Parboteeah, 2005).

Two vignettes are designed to represent two different situations. The first represents an innocuous-defined situation, while the other typifies a pernicious-defined situation. Although this approach has been adapted from Junglas and Spitzmuller (2005), they exposed each respondent to only one scenario. This research argues, however, that if respondents are exposed to only one version, then it might unfairly prompt a certain way of thinking from participants and, therefore, skew responses in a way that may undermine the validity of the survey results. Therefore, and since vignettes' information are one of the main basis for each respondent's choices, every participant will be provided with two vignettes that represent "the positive implications of LBS" and "the negative implications of LBS". Accordingly, presenting all sides of the issue is an attempt to achieve objectivity by controlling undue influence and avoiding inherent bias in the survey questions.

The third section of the survey is the questionnaire. The questionnaire itself contains a set of statements for each of the model's constructs. A set of Likert-type statements is developed for every composite construct. In order to increase constructs measurement reliability, most items, which have been fielded and validated in former studies were adapted to reflect the specific context of this research i.e. LBS.

The survey will target the people of Wollongong City, New South Wales, Australia. Wollongong is a diverse multicultural city with a population of more than 260,000 (Australian Bureau of Statistics, 2007). The main reason for selecting city-siders as the type of the survey's population is that they are more suitable representation of the of prospective "general users" of LBS than any other population types such as university students or professional users (King & He, 2006).

5 Conclusion

Wireless mobile technologies such as LBS have been exploited in several countries to complement traditional emergency systems. However, their utilisation in the domain of emergency management has not yet commenced in Australia. This paper is part of an ongoing investigation regarding the consequences of introducing LBS under an all-hazardous approach for managing natural and man-made emergencies. The study, in particular, investigates user acceptance of LBS, and examines the importance of user acceptance in deploying successful LBS solutions in Australia. A conceptual model has been theorised to better understand the underlying determinants that will influence users' perspectives. Citizen's user acceptance of LBS will be surveyed. The results are expected to confirm or refute the willingness of Australians in particular to use these services and provide an insight about the issues and concerns that general users might have.

References

Agarwal, R. 2000, 'Individual Acceptance of Information Technologies', in R.W. Zmud (ed.), *Framing the domains of IT management: projecting the future … through the past*, Pinnaflex Education Resources, Cincinnati, Ohio, pp. 85-104.

Agarwal, R. & Prasad, J. 1997, 'The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies', *Decision Sciences*, vol. 28, no. 3, pp. 557-582.

Al-Gahtani, S.S. 2002, 'Extending the Technology Acceptance Model beyond its Country of Origin: A Cultural Test in Western Europe', in M. Khosrowpour (ed.), *Advanced Topics information Resources Management*, Idea Group Publishing, Hershey, Pennsylvania.

Al-Gahtani, S.S. & King, M. 1999, 'Attitudes, satisfaction and usage: factors contributing to each in the acceptance of information technology', *Behaviour & Information Technology*, vol. 18, no. 4, pp. 277-297.

Aloudat, A., Katina, M. & Jun, Y. 2007, 'Location-Based Services in Emergency Management- from Government to Citizens: Global Case Studies', in P. Mendis, J. Lai, E. Dawson & H. Abbass (eds), *Recent Advances in Security Technology*, Australian Homeland Security Research Centre, Melbourne, pp. 190-201.

Australian Bureau of Statistics 2007, *The 2006 Census QuickStats : Wollongong (NSW) (Statistical District)*, viewed 04 February 2008 <http://www.censusdata.abs.gov.au/ABSNavigation/prenav/LocationSearch?collection=Census&period=2006&areacode=1006&producttype=QuickStats&breadcrumb=PL&action=401>.

Bauer, H.H., Barnes, S.J., Reichardt, T. & Neumann, M.M. 2005, 'Driving Consumer Acceptance of Mobile Marketing: A Theoretical Framework and Empirical Study', *Journal of Electronic Commerce Research*, vol. 6, no. 3, pp. 181-192.

Bulte, C.V.d. & Lilien, G.L. 2001, *Two-Stage Partial Observability Models of Innovation Adoption*, Working Paper, Wharton School, University of Pennsylvania, Philadelphia, viewed 04 August 2007.

Cho, Y.C. & Agrusa, J. 2006, 'Assessing Use Acceptance and Satisfaction Toward Online Travel Agencies', *Information Technology & Tourism*, vol. 8, pp. 179–195.

Code of Practice of Passive Location Services in the UK 2006, *Industry Code of Practice For the use of mobile phone technology to provide passive location services in the UK*, viewed 23 Aug 2007 <http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf>.

Cook, T.D. & Campbell, D.T. 1979, *Quasi-experimentation : design & analysis issues for field settings*, Rand McNally College Pub. Co., Chicago.

Davis, F.D. 1986, *A technology acceptance model for empirically testing new end-user iformation systems: theory and results*, Doctoral Dissertation, *MIT Sloan School of Management*, Massachusetts Institute of Technology, Cambridge, Massachusetts, viewed 4 September 2007.

Davis, F.D. 1989, 'Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology', *MIS Quarterly*, vol. 13, no. 3, pp. 318-340.

Davis, F.D. 1993, 'User acceptance of information technology: system characteristics, user perceptions and behavioral impacts', *International Journal of Man-Machine Studies*, vol. 38, no. 3, pp. 475-487.

Davis, F.D., Bagozzi, R.P. & Warshaw, P.R. 1989, 'User acceptance of computer technology: a comparison of two theoretical models', *Management Science*, vol. 35, no. 8, pp. 982-1003.

DeLone, W. & McLean, E. 2002, 'Information Systems Success Revisited', *the Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, vol. 8, IEEE Computer Society, viewed 2 December 2007.

Despont-Gros, C., Mueller, H. & Lovis, C. 2005, 'Evaluating user interactions with clinical information systems: A model based on human-computer interaction models', *Journal of Biomedical Informatics*, vol. 38, no. 3, pp. 244-255.

Dillon, A. 2001, 'User acceptance of information technology', in W. Karwowski (ed.), *Encyclopedia of Human Factors and Ergonomics*, Taylor and Francis, London.

Dillon, A. & Morris, M.G. 1996, 'User acceptance of new information technology - theories and models', in M. Williams (ed.), *Annual Review of Information Science and Technology*, vol. 31, Information Today, Medford, New Jersey, pp. 3-32.

Esrock, S.L. & Ferre, J.P. 1999, 'A Dichotomy of Privacy: Personal and Professional Attitudes of Marketers', *Business and Society Review*, vol. 104, no. 1, pp. 107-120.

Finch, J. 1987, 'Research note: the vignette technique in survey research', *Sociology*, vol. 21, no. 1, pp. 105–114.

Fishbein, M. & Ajzen, I. 1975, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley Publishing Company, Reading, Massachusetts.

Fisher, R.J. 1993, 'Social desirability bias and the validity of indirect questioning', *Journal of Consumer Research*, vol. 20, no. 2, pp. 303-315.

Hann, I.-H., Hui, K.-L., Lee, T.S. & Png, I.P.L. 2002, 'Online Information Privacy: Measuring the Cost-Benefit Trade-Off', paper presented to the *Twenty-Third International Conference on Information Systems*, Barcelona , Spain, December 2002.

Havlena, W.J. & Holbrook, M.B. 1986, 'The Varieties of Consumption Experience: Comparing Two Typologies of Emotion in Consumer Behavior', *Journal of Consumer Research*, vol. 13, no. 3, pp. 394-404.

Ho, S.Y. & Kwok, S.H. 2003, 'The attraction of personalized service for users in mobile commerce: an empirical study', *ACM SIGecom Exchanges*, vol. 3, no. 4, pp. 10-18.

Hoffman, D.L., Novak, T.P. & Peralta, M. 1999, 'Building Consumer Trust Online', *Communications of the ACM*, vol. 42, no. 4, pp. 80-85.

International Telecommunication Union 2002, *ITU Internet Reports: Internet for a Mobile Generation*, viewed 05 July 2008 <http://www.itu.int/wsis/tunis/newsroom/stats/Mobile_Internet_2002.pdf>.

Ives, B., Olson, M.H. & Baroudi, J.J. 1983, 'The measurement of user information satisfaction', *Commun. ACM*, vol. 26, no. 10, pp. 785-793.

Junglas, I.A. & Spitzmuller, C. 2005, 'A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services', *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Hawaii pp. 180b-180b, viewed 22 August 2007.

Kalish, S. 1985, 'A NEW PRODUCT ADOPTION MODEL WITH PRICE, ADVERTISING ,AND UNCERTAINTY', *Management Science*, vol. 31, no. 12, pp. 1569-1585.

Karahanna, E. 1999, 'Symbolic Adoption of Information Technology', *in the Proceedings of the International Decision Sciences Institute*.

King, W.R. & He, J. 2006, 'A meta-analysis of the technology acceptance model', *Information & Management*, vol. 43, no. 6, pp. 740–755.

Krishnamurthy, N. 2002, 'Using SMS to deliver location-based services', paper presented to the *Personal Wireless Communications*.

Küpper, A. 2005, *Location-based Services: Fundamentals and Operation*, John Wiley & Sons Ltd, Chichester, West Sussex.

Lee, S.M., Kim, Y.R. & Lee, J. 1995, 'An Empirical Study of the Relationships among End-User Information Systems Acceptance, Training, and Effectiveness', *Journal of Management Information Systems*, vol. 12, no. 2, pp. 189-202.

Liljander, V., Riel, A.C.R.v. & Pura, M. 2002, 'Customer satisfaction with e-services: the case of an on-line recruitment portal', in M. Bruhn & B. Stauss (eds), *Jahrbuch Dienstleistungsmanagement 2002 – Electronic Services*, Gabler, Wiesbaden, pp. 407-432.

Malhotra, Y. & Galletta, D.F. 1999, 'Extending the Technology Acceptance Model to Account for Social Influence:

Theoretical Bases and Empirical Validation', *Proceedings of the 32nd Hawaii International Conference on System Sciences*, Hawaii, USA, viewed 29 August 2007.

Martin, E. 2004, 'Vignettes and Respondent Debriefing for Questionnaire Design and Evaluation', in R.M. Groves, G. Kalton, J.N.K. Rao, N. Schwarz & C. Skinner (eds), *Methods for Testing and Evaluating Survey Questionnaires*, John Wiley & Sons, Inc., Hoboken, New Jersey.

Mayer, R.C., Davis, J.H. & Schoorman, F.D. 1995, 'An Integrative Model of Organizational Trust', *Academy of Management Review*, vol. 20, no. 3, pp. 709-734.

Michael, A. & Salter, B. 2006, *Mobile Marketing: Achieving Competitive Advantage Through Wireless Technology*, 1st edition edn, Butterworth-Heinemann, Elsevier Ltd., London, UK.

Michael, K., Perusco, L. & Michael, M.G. 2006, 'Location-Based Services and the Privacy-Security Dichotomy', *Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking*, London, pp. 91-98, viewed 26 May 2007.

Morris, J.B. 2002, 'The Elements of Location Tracking and Privacy Protection', in B. Sarikaya (ed.), *Geographic location in the Internet*, Kluwer Academic Publishers, Boston, pp. 163 - 178.

Morrison, R.L., Stettler, K. & Anderson, A.E. 2004, 'Using vignettes in cognitive research on establishment surveys', *Journal of Official Statistics*, vol. 20, no. 2, pp. 319-340.

Oxford University 2002, *Oxford English Dictionary*, in J. Simpson, E. Weiner, M. Proffitt, A. Hughes, Y. Warburton, P. Gilliver, J. Paterson & S. Tulloch (eds), *OED*, 2nd edn, vol. 3, Oxford University Press, London.

Parasuraman, A., Berry , L. & Zeithaml, V. 1988, 'SERVQUAL: A multiple-item scale for measuring service quality. Journal of Retailing', *Journal of Retailing*, vol. 64, no. 1, pp. 12-40.

Parasuraman, A., Zeithaml, V., A. & Malhotra, A. 2005, 'E-S-QUAL: A Multiple-Item Scale for Assessing Electronic Service Quality', *Journal of Service Research : JSR*, vol. 7, no. 3, p. 213.

Parboteeah, D.V. 2005, *A Model of Online Impulse Buying: An Empirical Study*, Doctoral Dissertation, *Department of Information Systems*, Washington State University, Washington, p. 360, viewed 27 October 2007.

Pavlou, P.A. 2003, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model', *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-134.

Pavlou, P.A. & Gefen, D. 2004, 'Building Effective Online Marketplaces with Institution-Based Trust', *Information Systems Research*, vol. 15, no. 1, pp. 37-59.

Presser, S., Couper, M.P., Lessler, J.T., Martin, E., Martin, J., Rothgeb, J.M. & Singer, E. 2004, 'Methods for Testing and Evaluating Survey Questions', *Public Opinion Quarterly*, vol. 68, no. 1, pp. 109-130.

Rawstorne, P. 2005, *A Systematic Analysis of the Theory of Reasoned Action, the Theory of Planned Behaviour and the Technology Acceptance Model When Applied to the Prediction and Explanation of Information Systems Use in Mandatory Usage Contexts*, Doctoral Dissertation, *The Department of Psychology*, University of Wollongong, Wollongong, viewed 10 October 2007.

Saadé, R.G. & Kira, D. 2006, 'The Emotional State of Technology Acceptance', *in the Proceedings of of 6th Informing Science and IT Education Conference*, vol. 3, Informing Science Institute, Manchester, England, viewed 11 November 2007.

Scharl, A., Dickinger, A. & Murphy, J. 2005, 'Diffusion and success factors of mobile marketing', *Electronic Commerce Research and Applications*, vol. 4, no. 2, pp. 159-173.

Schoenberg, N.E. & Ravdal, H. 2000, 'Using vignettes in awareness and attitudinal research', *International Journal of Social Research Methodology*, vol. 3, no. 1, pp. 63-74.

Swanson, E.B. 1988, *Information System Implementation: Bridging the Gap Between Design and Utilization*, Irwin, Homewood, Illinois.

Taylor, S. & Todd, P. 1995, 'Understanding Information Technology Usage: A Test of Competing Models', *Information Systems Research*, vol. 6, no. 2, pp. 144-176.

Venkatesh, V. & Brown, S.A. 2001, 'A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges', *MIS Quarterly*, vol. 25, no. 1, pp. 71-102.

Weenig, M.W.H. & Midden, C.J.H. 1991, 'Communication Network Influences on Information Diffusion and Persuasion', *Journal of Personality & Social Psychology*, vol. 61, no. 5, pp. 734-742.

Weiss, D., Kramer, I., Treu, G. & Kupper, A. 2006, 'Zone Services - An Approach for Location-Based Data Collection', paper presented to the *The 8th IEEE International Conference on E-Commerce Technology, The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services*.

Wilks, T. 2004, 'The Use of Vignettes in Qualitative Research into Social Work Values', *Qualitative Social Work*, vol. 3, no. 1, pp. 78-87.

Xu, H. & Teo, H.-H. 2004, 'Alleviating Consumer's Privacy Concerns in Location-Based Services: A Psychological Control Perspective', *the Twenty-Fifth Annual International Conference on Information Systems (ICIS)*, Washington, D. C, pp. 793-806, viewed 20 August 2007.

Xu, H. & Teo, H.-H. 2005, 'Privacy Considerations in Location-Based Advertising', in C. Sørensen, y. Yoo, K. Lyytinen & J.I. DeGross (eds), *Designing Ubiquitous Information Environments: Socio-Technical Issues and Challenges*, vol. 185, Springer, Boston, pp. 71-90.

Xu, H., Teo, H.-H. & Tan, B.C.Y. 2005, 'Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk', paper presented to the *Twenty-Sixth International Conference on Information Systems*, Las Vegas, USA, 11-14 December

Yang, Z., Peterson, R.T. & Cai, S. 2003, 'Services quality dimensions of Internet retailing: an exploratory analysis', *Journal of Services Marketing*, vol. 17, no. 7, pp. 685–700.

Zeithaml, V.A., Parasuraman, A. & Malhotra, A. 2000, *A Conceptual Framework for Understanding e-Service Quality: Implications for Future Research and Managerial Practice: Working paper*, *Cambridge MA, Marketing Science Institute*, viewed 09 November 2007.

Zweig, D. & Webster, J. 2002, 'Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems', *Journal of Organizational Behavior*, vol. 23, no. 5, p. 605.

16

Profiting from personal information: Power, information privacy and evidence based policy

Mark Burdon

PhD Candidate/Research Associate, Faculty of Law/Information Security Institute, Queensland University of Technology

Abstract

The difficulties that emerge when governments attempt to commercialise personal information are shown by the sale of home owner details in Queensland. Solove contends that such difficulties arise because of power differences between government organisations, private sector companies and individuals. The development of effective policy responses, particularly those regarding the sale of personal information, must identify and address power issues inherent in information privacy problems.

Keywords: information privacy, power, decision making, accountability, transparency

1 Introduction

The public sector has a large number of databases containing personal data such as names, addresses and ages. In the UK, it has been estimated that there are 300 million personal data records – on average five sets of personal data for every citizen (Council for Science and Technology 2005, 6). This highlights the unique position that governments have as the primary collector of public data (OECD 2006). Government organisations have statutory means to enforce disclosure and they are the only feasible provider of comprehensive national data sets (Rowlands 1995, 227). Concurrently, the enhanced development of information and communication technologies in government has created new opportunities for agencies to collect, share and re-use data. As a consequence, the commercial worth of governmental data sets and value added information products/services have increased (PIRA International 2000). Government organisations are now finding that data which they have routinely collected to fulfil their statutory and business functions can now more easily be re-used for commercial purposes (Office of Fair Trading 2006). As such, the commercialisation of public sector information, including personal information, has been a part of the developing information economy which is believed to generate annual worldwide revenues in the hundreds of billions of dollars (Somogy 2006, 904).

However, the commercialisation of personal information by governments can create information privacy problems as highlighted in the next section. Solove argues that such problems occur from the imbalance of power relationships between individuals and organisations. Section 3 examines Solove's claims and Section 4 applies his analysis to the Queensland problem. Section 5 looks further into the relationship between power and privacy and suggests that a different form of policy research could be used for evidence based policy development. Finally, the author briefly concludes the paper about how such an approach could help to factor in underlying power mechanisms involved in information privacy problems and thus lead to the further development of information privacy laws.

2 A Queensland information privacy problem arising from the sale of personal information

The recent Federal Court case of *RP Data v State of Queensland [2007] FCA 1639* highlights some major concerns for government organisations regarding the re-use of personal information for income generation purposes. The Department of Natural Resources and Mines (now Department of Natural Resources and Water and hence referred to as NRW) is mandated by law to collect and maintain information on real property valuations arising from obligations under the Valuation of Land Act (QLD) 1994 (hence referred to as the VLA) and land title information under the Land Titles Act (QLD) 1994. Section 37 of the VLA requires NRW to conduct an annual valuation of the unimproved value of all land in local government areas and to record details of valuation in a roll. The valuation roll contains information such as a property owners name and address; the situation, description and measurement or area of the land; a valuation of the unimproved value and additional details required under section 47 of the VLA.

Further statutory requirements arising from the VLA also oblige NRW to supply valuations data in various forms. For example, section 73 requires the Chief Executive of NRW to provide a copy of the valuation roll to various administrative parties such as the Commissioner of Land Tax. Section 77 of the VLA establishes the context in which NRW can sell valuation information. The Chief Executive is entitled to embark on contractual relations with third parties for the supply of valuation roll information in the form of bulk data products. For the purpose of the legislation, bulk data is defined as at 20% of all land parcels in Queensland or all section 81 information for parcels of land in Queensland.

NRW combined the valuations data with data collected on property sales to create the Queensland Valuation and Sales (QVAS) dataset which was first supplied under licence to RP Data, an information broker, in 1992. RP Data was one of eight information brokers used by NRW to distribute QVAS but it was by far the biggest with a 70% share of the information market. RP Data was effectively a non-exclusive data broker for NRW and value added the QVAS data into a more commercially friendly product that was sold, predominantly to real estate agents, but also to other government departments. Interestingly, at the onset of the relationship, RP Data informed NRW of the possibility that value added information may be used for direct marketing by real estate agents and the agency was prepared to contemplate that use. However, this was not the case 10 years later, when NRW sought a change of policy.

During the intervening years, NRW received a number of complaints regarding the use of personal information provided to the agency that had been re-used by real estate agents for direct marketing purposes. This led to the instigation of section 27 of the Land Legislation Amendment Act (QLD) 2003 which sought to prohibit the use of direct marketing, using names and addresses supplied by NRW in the QVAS dataset. Section 27 inserted two subsections into the VLA. Section 77(3)(A)(a) allowed the Chief Executive of NRW to exclude elements of the valuation roll information provided under contract if he/she ""is satisfied, on reasonable grounds, that inclusion of the particulars may result in the particulars being inappropriately disclosed or used". Section 77(3)(A)(b) provided a retrospective power to prohibit disclosure or limit distribution and use of supplied information.

The advent of section 77(3)(A) led to a new licensing agreement between NRW and the 8 information brokers which came into effect in July 2003. The new licence had four new clauses that directly prohibited direct marketing of NRW's QVAS dataset. Clause 4.4.2 required the licensee to acknowledge and to be bound by restrictions that did not allow licensed data, consisting of details identifying individuals (e.g. names and addresses), to be used for direct marketing. Clause 4.5.2 required the licensee not to distribute the licensed data to a third party for direct marketing purposes. Furthermore, clauses 4.10.2 and 4.11 required that the licensee must not distribute the licensed data to an end user unless that party has entered into an agreement not to use the data for direct marketing. Finally, clause 9.11 affirmed the right of the licensor to exclude elements of QVAS data on reasonable grounds of inappropriate use or disclosure (e.g. direct marketing).

Despite the new licensing agreement, the QVAS data continued to be used by real estate agents for direct marketing purposes and NRW received 219 written complaints and numerous phone calls from members of the public. Additional complaints were also received by real estate agents who were 'doing the right thing' by adhering to NRW's licence requirements and managing agents of unit complexes. The lack of compliance with the new licence prompted NRW in July 2005 to exclude the provision of names and addresses in the QVAS dataset. The purpose of which was explained by NRW's Director of Product Services in his affidavit to the court:

> "15. The purpose of making a new proposal to withdraw names and addresses from the bulk data was as a consequence of complaints received from various individuals that their personal details had been obtained by direct marketers and they were concerned about Government information being used in inappropriate ways."

RP Data then brought an action against NRW under section 46 of the Trade Practices Act (Cth) 1974 on the grounds that NRW had abused its market power by withdrawing names and addresses from QVAS. The grounds of the action are beyond the scope of this paper but it is worth noting that judgment was found for NRW on the basis that the removal of names and addresses was not based on anti-competitive behaviour but on a desire to ensure that NRW's information was not used improperly.

It is somewhat surprising that concerns about the commercialisation of personal information have not come to the fore at an earlier stage. Larson (1994, 40-44) highlights that the re-use and sale of census data in the US started in the late 1960's and was a major contributing factor to the development of direct marketing tactics. Large-scale, publicly collected datasets were merged and re-formatted into new mailing lists, used specifically for targeting customers and sending mail shots. Moreover, recent research conducted for the UK Government has suggested that formal information privacy principles are required to ensure the governance of enhanced information sharing. As a consequence, government organisations should not be allowed to sell public sector personal information to commercial organisations (OPM 2005, 14). However, identifying the actual causes of such problems and anxieties are perhaps not as clear cut as can first appear due to the inherent issues of power underlying the relationship between individuals and bureaucracies that are manifest in information privacy concerns.

3 Metaphors of power

Solove (2001) contends that information privacy problems, similar to those encountered in Queensland, are best explained as arising from unbalanced power relationships between individuals and organisations. More specifically, issues of mass personal data collection are grounded in an outdated paradigm of information privacy as a Big Brother problem. This metaphorical view, based on Orwell's '1984', depicts privacy problems as invasions of privacy through surveillance. Or in the context of databases, through 'dataveillance' (Clarke 2006) which is the systematic collection and use of personal and non-personal data by bureaucracies for surveillance purposes (Solove 2001, 1417). Whilst this view has been dominant amongst most privacy legal theorists and law makers, Solove contends that a more appropriate metaphor, to view privacy problems arising from the use of databases, emerges from a view of privacy based on Kafka's 'The Trial'.

The Big Brother metaphor provides a narrow view of the application of information privacy in society. In 1984, the fictional state of Oceania is dominated by an omnipotent and all knowing governmental bureaucracy encapsulated by its dictator leader, Big Brother. Each citizen's life is strictly regulated as Big Brother controls all aspects of existence. Collective uniformity is gained through absolute obedience founded on fear of punishment and execution. The concept of personal privacy is eradicated as Big Brother exercises power through constant surveillance via the obsequious 'telescreen' thus leading to the elimination of private thoughts. Privacy using the Big Brother metaphor therefore represents the use of coercive power by governments to oppress, control and dominate (Solove 2001, 1415).

Solove argues that the Kafka metaphor offers a more realistic analysis of the information privacy concerns relating to databases and the power issues entailed. In The Trial, an individual, Joseph K is notified that he has been arrested for an unnamed offence. Outraged and perplexed, he embarks on a quest to ascertain why he has been arrested and who is behind his arrest. Joseph K encounters a bureaucratic legal system that is indifferent to the needs of individuals, is devoid of purpose and exercises power for no apparent goal or reason (Solove 2001, 1423). In real life, Solove contends that the primary information privacy problem with databases stem from the way the bureaucratic process treats individuals and their information (Solove 2001, 1421). Especially bureaucracies and bureaucratic processes that have little intelligent control or limitation which result in a lack of meaningful participation by individuals regarding the decisions to collect and use their personal data (Solove 2001, 1422).

There are significant differences between conceptualisations derived from both the Big Brother and Kafka metaphors. However, the use of both metaphors conceives information privacy issues as problems of power. The Big Brother metaphor is concerned with the direct exercise of power by bureaucratic organisations to coerce individuals. Power in the Big Brother sense involves dictatorship, control and enforced obedience. Whereas the Kafka metaphor focuses on the imbalance of power relationships between helpless individuals and uncaring bureaucracies that make decisions and enact without any meaningful purpose or design. Under the latter, Solove is referring to the information privacy dangers arising from neglectful, ill-conceived and disempowering administrative practices that govern the collection, storage and use of personal data. Solove's metaphorical analysis of information privacy as power is particularly pertinent to the issue of the re-use of personal information, held by government agencies, for income generation purposes. In terms of the commercialisation of personal information, such actions highlight the complex and shifting balance of power relationships between government departments, data brokers, commercial entities and individuals. The next section will apply Solove's metaphors to the Queensland example highlighted above to outline the operation of power relationships emanating from information privacy problems arising from the sale of personal information.

4 A power analysis of the Queensland example

Using Solove's metaphors, it would appear that the problem highlighted above is much more akin to a Kafka rather than a Big Brother type concern. The sale of the QVAS dataset by NRW and the subsequent purchase and re-use by RP Data was not conducted for reasons of surveillance and was not intended to impose control of those persons who provided their personal information. The overt focus on surveillance intrinsic in the Big Brother metaphor ignores the practical reasons that the majority of personal data is collected for. Bureaucratic personal data collection is not purely aimed at gaining control over a populace. Instead, the goal of much personal data collection, particularly its use by the private sector, is aimed at studying and exploiting our expressions of individuality rather than attempting to suppress them (Solove 2001, 1419). This point can be seen clearly in the re-use of the QVAS dataset by RP Data and estate agents, which was used for commercial purposes (e.g. direct marketing) rather than oppressive attempts of control.

Solove also contends that bureaucratic personal data collection and use is conducted by a myriad of 'Little Brothers' (Lyon 1994) for a wide-range of purposes rather than by one omnipotent government agency for one purpose (Solove 2001, 1421). Solove argues that the world is essentially controlled by bureaucracies and the important factor to be considered regarding the collection of personal data is the relationship between individuals, society and the 'Little Brothers'. Bureaucratic databases, and the data held in them, are integral to government and commercial decision-making, and to that extent, exacerbate and transform the power relationships between individuals and bureaucracies (Solove 2001, 1422). This diffusion of data collection and use highlights the fact that the majority of personal data collected does not actually have an embarrassing element and that most people are happy to part with seemingly innocuous personal details. The Queensland example re-emphasises this point. The primary act of data collection was done so by NRW under the auspices of the VLA that compelled individuals to provide personal data and mandated the agency to collect it. It was not until the subsequent re-use of the primary personal data, first by NRW to produce the QVAS dataset and then by RP Data and real estate agents, for commercial purposes that the provision of "seemingly innocuous personal details" was suddenly perceived in a new light.

This highlights that information privacy problems occur from a group of disempowering practices associated with the collection and use of personal data (Solove 2001, 1425). Solove argues that a precondition for successful information privacy regulation must be to establish rules that govern the power relationships between individuals and bureaucracies (Solove 2001, 1455). Such rules should seek to equalise power imbalances and thus ensure the instigation of fair, voluntary and informed information transactions. In the Queensland example, it would appear that these rules were not given enough weight by the organisations involved. Complaints from individuals did not emanate until certain acts of re-use, i.e. direct marketing, started to attract the annoyance of those persons who provided their personal information for a specific purpose only for it to be used later for a totally different purpose.

For Solove, the information privacy problems arising from mass personal data collection and the use of bureaucratic databases regard the power relationships between individuals, societies and bureaucratic organisations. Particularly as the relationship an individual has to a bureaucracy, even a benign one, about the data collected from and about them, can have a potentially debilitating effect (Solove 2001, 1423). An interesting point that arises from the Queensland example is the fact that, at various stages of the problem, NRW was powerless to stop the re-use of personal information held in their possession for direct marketing. At those times, the government organisation was debilitated as well as the individuals in question. This highlights the complex web of power relations between 'Little Brothers' and individuals in which all parties exerted some form of power over the others. For example, individual complaints made NRW take action to withdraw personal information from RP Data, who in turn, was not able to use the QVAS dataset for the development of information products for real estate agents. Accordingly, all parties appear to have been able to exert power over the others at varying stages in the episode.

In some ways, this goes beyond traditional notions of information privacy that focus on one-to-one relationships of control over information that have been shaped within a property rights paradigm revolving around notions of ownership of personal data (Solove 2001, 1446). Solove argues that the use of this paradigm has skewed perspectives of information privacy because it focuses on balancing competing economic values between the bureaucratic organisation, that collects and holds the information; the value an individual puts on the information and the larger social value of individual's maintaining control of their information (Solove 2001, 1446). This point can be seen clearly in the Queensland example. The problem appears to have emerged due to a combination of certain factors: (a) NRW's original decision to commercialise information, including personal information (b) individuals were not informed that their personal information was being sold (c) the subsequent re-use of personal information, by another body, for direct marketing purposes. It would appear that at various stages, the economic considerations of those organisations involved outweighed the societal value of maintaining control of personal information. It is not until the point where individuals start to value the use of their personal information that the latter, at least in terms of NRW's involvement, started to outweigh the former.

5 Power, information privacy and evidence based policy

Once the notion of power as an element of information privacy is applied, the underlying foundations of information privacy law no longer appear suitable to resolve current and future problems because of the dominant paradigms of surveillance and ownership which continually divert attention away from the real problem - the imbalance of power relationships (Solove 2001, 1431). However, like privacy, the concept of power has been notoriously difficult to define (Lukes 2005, 61; Dyrberg 1997, 1) which is why it has perhaps received so little academic discussion in the US and in Australia.

Ehrenreich (2001) argues that power has not been discussed in tandem with privacy because of the imprecise nature of power, particularly in the form of Marxist discourse, that has largely been discredited in the US (Ehrenreich 2001, 2057). As a result, to speak of power in modern America is akin to saying something distasteful because it reminds Americans of inequalities that they would rather not acknowledge. Power is hard to talk about, but privacy is not because "the notion of privacy resonates well in a country so heavily seduced by the notion of 'individual freedom'" (Ehrenreich 2001, 2057). It is difficult for the American political discourse to distinguish fully between privacy and power because both concepts are so intimately bound together (Ehrenreich 2001, 2058)

> "[I]t would probably not be an exaggeration to say that without privacy, power could not sustain itself; and without power, privacy could not exist. As I argue in the remainder of this Review Essay, the realm of the "private" is always constructed in relation to social power: Power constructs privacy and, to maintain itself, power also destroys privacy. Privacy, in turn, both constructs power and challenges it."

As regards the Australian literature, Lindsay (2005) has addressed Foucauldian concepts in the wider context of Australian information privacy laws and contests that the issue of power and privacy has yet to be fully explored (Lindsay 2005, 140). He argues that Foucault's analysis of power may assist in explaining some of the difficulties encountered with defining the concept of privacy (Lindsay 2005, 139). In so doing he defines Foucault's conception of power as

> "In his [Foucault's] view, conceiving power solely in terms of a struggle between state repression and individual liberties ignores more insidious

techniques through which power is exercised in everyday life" (Lindsay 2005, 138).

Power is not purely about negative applications in the form of repression. Foucault's contention is that power can also have a positive effect because it can be used to produce knowledge and facilitate discourse. Lindsay states that Foucauldian notions of power are relevant to information privacy concerns because they highlight that the concept of privacy is really "concerned with techniques of power that are dispersed within society, and which takes a diversity of forms" (Lindsay 2005, 139). As such, "if power relationships are everywhere, then privacy, which must be seen in the context of such relations, is an understandably diffuse concept, capable of multiple meanings" (Lindsay 2005, 139).

This raises a number of challenges for evidence based policy about information privacy problems arising from the sale of personal information and such problems generally because of the invisible and conflicting nature of one of the potential causes – underlying power relationships. Policy responses therefore have to pay regard to the limits of traditional ontological and epistemological assumptions about the nature of social reality which dictate the methods of knowledge acquisition. Put simply, if underlying power relations are not conceived as a cause of information privacy problems then they will never be identified as such. Legislative and policy responses will continue to be developed but they may not be effective because one of the main underlying issues, is at best, addressed in a tangential manner. What is required, therefore, is a way of thinking about policy problems that is able to identify and address invisible causal mechanisms, such as power, that are fundamental to resolving the concern at heart.

Pawson and Tilley (1997) have applied a critical realist approach to examine policy responses implemented to reduce car park crime through the use of closed circuit TV (CCTV) cameras. Critical realist research builds models of mechanisms to be adopted as hypothetical descriptions used to reveal underlying causal mechanisms (Blaikie 2006). The research task is to demonstrate the existence of the explanatory mechanisms postulated and explanation is constructed in terms of how causal mechanisms produce events (Blaikie 2000). The guiding metaphors are therefore structures and mechanisms of reality rather than the rigorous observation of a phenomenon or event (Robson 2002, 32).

The authors argued that the use of CCTV cameras in car parks worked, not because of their presence alone, but because they triggered a chain of reasoning and response in the minds of would be thieves that inhibit illegal actions (Pawson and Tilley 1997, 78). The purpose of realist evaluation is therefore to develop a comprehensive theory of how the implementation of CCTV impacts on the thought process of the criminal mind and what combination of causal mechanisms and actual contexts produce the most effective inhibitor to car park crime. For example, CCTV could reduce car park crime because it (a) makes it more likely that an offender will be observed (b) may produce evidence that can be used in a future court action; (c) allows security resources to be allocated immediately and more effectively; or (d) may appeal to drivers to be extra vigilant regarding the security of their vehicle.

It is also possible for other causal mechanisms to exist and it is also possible that these and other mechanisms can exist at the same time. Which particular mechanism or combination of mechanisms most influences the criminal mind in turn may depend on the context for which the CCTV is installed (Pawson and Tilley 1997, 79). For example, if the car park is isolated and has little or no security, the ability to apply resources immediately is diminished and the car park operators are more reliant upon the deterrent of being able capture criminal activity on camera. This clearly provides a more limited response in contrast to a busy, security resourced car park because the latter offers a greater number of mechanisms that can inhibit the potential car thief by influencing their thought patterns. The authors contend that such an approach reveals that a bit of lateral thinking in the realm of hypothesis making frames the search for data and the application of research strategies and thus call upon the use of a range of evidence entirely different from traditional methods (Pawson and Tilley 1997, 80).

A similar approach to Pawson and Tilley's could be applied to information privacy policy evaluation to assist the identification of power mechanisms as a cause of information privacy problems, particularly those arising from the sale of personal information. Policy makers and policy analysts would be required to search for different forms of evidence that go beyond the implementation of information privacy laws and simple measurement of outcomes, generally in the form of legal actions or complaints. Instead, a much deeper evidential search would be required to examine the effects of unbalanced power relationships on the interplay between the providers, collectors and users of personal information.

The acquisition of new evidence could unveil the complex interplay of hidden mechanisms involving individuals and organisations, such as the demands for governments to be economically self-sufficient, the increasing value that the information market puts on personal information and the angst that is generated when personal information is used beyond the bounds that it is collected for, particularly direct marketing. Ultimately, this could show the limits of current information privacy laws that are founded on notions of ownership and which do not sufficiently acknowledge the existence of the power relations that are intrinsic to information privacy issues.

6 Conclusion

This paper has sought to highlight the relationship between power and information privacy within the context of an information privacy problem arising from the sale of personal information. Such issues and the relationships entailed are clearly complex given the amorphous nature of both concepts. The effective resolution of information privacy problems, such as the one highlighted above, requires policy responses that consider new ways of thinking to address underlying causes particularly those that emerge from power imbalances.

A new way of thinking about the causes of information privacy problems could ultimately result in laws that develop informed disclosure by organisations which are founded on meaningful participation by individuals and go beyond notions of individual or corporate information ownership. It is therefore important that the development of information privacy laws focus on the structure of power in modern society and how to govern power relationships between individuals and bureaucracies regarding the collection and use of personal data. As Solove (2001, 1461) comments,

> "The problem with databases is not our being watched, controlled, or inhibited. Nor is it our lack of ownership in our personal information. Rather, it is a problem that involves power and the effects of our relationship with public and private bureaucracy - our inability to participate meaningfully in the collection and use of our personal information. As a result, we must focus on the structure of power in modem society and how to govern such relationships with bureaucracies."

References

Blaikie, N. 2000. *Designing Social Research: the Logic of Anticipation*. Cambridge, UK; Malden, MA: Polity Press.

Blaikie, N. 2006. *Approaches to Social Enquiry: Advancing Knowledge*. Cambridge, UK: Polity Press.

Clarke, R. 2006. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (accessed 30 April, 2007).

Council for Science and Technology. 2005. Better Use of Personal Information: Opportunities and Risks. London, UK: Council for Science and Technology.

Dyrberg, T. B. 1997. *The Circular Structure of Power: Politics, Identity, Community*. London; New York: Verso.

Ehrenreich, R. 2001. Privacy and Power. *Georgetown Law Journal*, 89 (6): 2047-2062.

Larson, E. 1994. *The Naked Consumer: How Our Private Lives Become Public Commodities*. New York: Penguin.

Lindsay, D. 2005. An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review* 29 (1): 131-178.

Lukes, S. 2005. *Power: A Radical View*. 2nd ed. Houndmills, Basingstoke, Hampshire: New York: Palgrave Macmillan.

Lyon, D. 1994. *Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

OECD. 2006. OECD Workshop on Public Sector Information: Summary: DSTI/ICCP/IE(2006)14.

Office of Fair Trading. 2006. The Commercial Use of Public Information (CUPI). London: Office of Fair Trading.

OPM. 2005. Research into the Use of Personal Datasets Held by Public Sector Bodies. London, UK: Council for Science and Technology.

Pawson, R. and N. Tilley. 1997. *Realistic Evaluation*. London; Thousand Oaks, Calif.: Sage.

PIRA International. 2000. Commercial Exploitation of Europe's Public Sector Information – Final Report. Leatherhead, Surrey, UK: European Commission, Directorate General for the Information Society.

Robson, C. 2002. *Real World Research: A Resource for Social Scientists and Practitioner-researchers*. 2nd ed. Oxford; Malden, Mass.: Blackwell Publishers.

Rowlands, I. 1995. Toward Public-Private Synergy in the European Information Services Market. *Journal of Government Information*, 22 (3): 227-235.

Solove, D. J. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, 53 (6): 1393-1462.

Somogy, D. J. 2006. Information Brokers and Privacy. *I/S: A Journal of Law and Policy for the Information Society*, 1 (2/3): 901-925.

17

The state of public data availability in Australia: A study of suppliers of critical infrastructure information

Roba Abbas

Graduate, School of Information Systems and Technology, Faculty of Informatics, University of Wollongong

Abstract

The purpose of this study is to evaluate the public data availability situation in Australia, and the consequent impact on the nation's critical infrastructure (CI) and the critical infrastructure protection (CIP) process in general, through an evaluation of data supplying bodies in Australia. An assessment of data suppliers was conducted, in order to allow for the categorisation of data supplying entities, and to identify the critical infrastructure data that is available. The public data availability situation in Australia is described, and the concerns associated with having CI-related information available in the public domain are highlighted.

Keywords: public data, critical infrastructure protection, threat, risks, information

1 Introduction

Critical infrastructure protection (CIP) has been a global concern since the Cold War. However, the issue has gained increased prominence in Australia since the incidents ofY2K, September 11 and Bali 2002 (Luiijf and Klaver, 2004; Emergency Management Australia, 2003). Additionally, the importance and increased use of the Internet and Information and Communication Technologies (ICT) have amplified the risks on critical infrastructure items (Popp et. al., 2004). These technologies provide outlets for data/information exchange, and have simplified the ability to transmit and access data; in particular, 'sensitive but unclassified' data that, when combined, enable inferences or previously undesired patterns to emerge.

Traditionally, the focus of CIP has been on the three major stages of vulnerability identification, risk assessment and risk management. A study conducted by Breeding in 2003 introduced the risk of 'sensitive but unclassified' data to America's infrastructure, viewing the threat on CIP from an alternative viewpoint. 'Sensitive but unclassified' data refers to information that may not on its own appear harmful, but when amalgamated with additional data elements can be truly revealing about CI. The outcomes of Breeding's research indicated that openly available information concerning America's critical infrastructure could prove damaging, in that they allow inferences to be made, which could consequently compromise any protection efforts by providing valuable details relating to the weak points and interdependencies between infrastructure items.

The purpose of this study, conducted in late 2006, was to adapt Breeding's process to an Australian setting, by identifying the public data suppliers in Australia, and consequently the amount of data that can be gathered in the public domain relating to Australia's CI. A public data supplier in this instance refers to any individual, institution or body that supports or facilitates the open distribution and use of information concerning Australia's critical infrastructure. The data may be deliberately or indirectly provided. Of particular importance to this paper are the identification of relevant data sources, and the classification of the types of information that exist in the public domain.

2 The data collection process

Data can be categorised in many ways. This study is focused specifically on free and commercial public data, which can be accessed physically and/or online, and includes multiple formats such as images, text, video, maps, geographic coordinates and statistics. The data of interest is critical infrastructure-related data, which refers to data that reveal certain aspects about Australia's critical infrastructure. The aim of this research was primarily to collect CI-related public data from data supplying agencies in Australia, utilising an Internet-enabled computer, and word processing and spreadsheet software as the primary tools for collection. The initial stages of the study included the identification and categorisation of data supplying entities, after which a repository was created using the available data from the identified agencies.

3 Data supplier categories

An assessment of the CI-related public data landscape in Australia enabled the identification of a number of distinct data supplier categories. The classes primarily include the individual/physical data collection, Government bodies, commercial suppliers, and other entities such as utility companies and telecommunications providers.

An interesting observation made throughout this study is that a majority of the supplying bodies enable free access to information, in an attempt to increase knowledge and educate their intended audience. This can be referred to as an optimistic view of data provisioning, in that the data is provided merely as a tool to assist individuals in better accomplishing certain tasks. The potentially undesirable consequences are therefore disregarded to an extent.

The subsequent sections provide an introduction to each data supplier category, including an evaluation of the types of data that were obtained while profiling the suppliers.

4 The individual/physical

The *individual/physical* represents first-hand data collection, where an individual independently collects critical infrastructure data from their surroundings. It is perhaps the simplest method of data gathering and access, as in most cases it does not require the assistance of a third party that may influence or prohibit the collection process. Certain data may require the use of entities such as libraries, Councils and information desks; however, others such as the capturing of video, photographs, GPS points and audio are independent activities. Publicly available critical infrastructure data that may physically be collected includes: tourist guides/brochures; hardcopy statistics, books and magazines; maps; photographs; video and audio recordings; and geographic coordinates using a Global Positioning System (GPS) tool.

First-hand data collection may be considered the simplest method of data gathering, given that in most instances there are very few mechanisms in place to screen the individual gathering the data. Additionally, once the data has been collected, there are minimal (and almost non-existent) enforcement techniques that govern the manner in which the critical infrastructure data may be used.

This source of public data collection was included in the scope of the study to ensure its completeness. However, it is difficult to practically introduce stringent security mechanisms to prevent such data from being accessed. To do so would completely compromise the basic principles of a trusting and informative society and community. As a result, the focus of the remainder of this paper is on electronic public data access, which is facilitated by the supplying agencies discussed below.

5 Federal and State Government departments

Government departments in Australia are prominent suppliers of public data due chiefly to their focus on providing an open and accessible data network through an electronic-Government (or e-Government) portal.

The e-Government movement of recent years has resulted in the trend to provide effortless access to information, in addition to the need to process information in an electronic environment (Wunnava and Reddy, 2000). e-Government "refers to the use of ICTs to promote more efficient and effective government services, allow greater public access to information and make government more accountable to citizens" (Punia and Saxena, 2004, p. 500). Many western countries such as Britain, Canada, the United States, and most notably Australia have been actively involved in e-Government initiatives since the mid-1990s (Lee et. al., 2005).

Traditionally, the aim of e-Government was to allow the public to monitor the activities of its government. However, authors such as Givens (n.d.) feel that e-Government is now centred on public records access, resulting in a number of negative implications. That is, the available records may be used for secondary purposes, such as to make inferences and perform data mining activities, which can reveal undesired patterns about entities. However, positive implications do exist and signify a more informed and knowledgeable public, and a certain level of trust between Government and citizens, which is a desired and productive outcome. However, as Givens (n.d.) states, the negative consequences must also be addressed.

The Australian Government is becoming progressively sophisticated in its provision of e-Government services, with government departments at all levels moving towards interactive services delivery (Davey, 2005). Additionally, the number of citizens making use of the electronic portal is increasing, which is greatly attributed to the advanced and information-rich web pages.

Given this concept of e-Government, this study involved an examination of the Australian Government portal (Australia.gov.au), and its link with other CI-related Australian Government departments. Australia.gov.au provides a gateway that connects the government with Australian citizens; "It links to information and services on over 700 Australian Government websites as well as selected state and territory resources. Australia.gov.au also searches over five million government web pages" (Australian Government, 2006).

Australia.gov.au was utilised as an initial point of analysis; that is, it was used to locate independent government agency websites, and to profile each department with respect to the available critical infrastructure information.

Notably, this study involved identifying Federal and State Government departments that provide information relating to Australia's Critical Infrastructure, and profiling the websites of the respective agencies. These agencies are identified in Figure 1. At the State Government level, New South Wales (NSW) was used as a representative example (case study), as it was not feasible at the time of the study to extend the scope to include all Australian states and territories.

The Government data collection process highlighted the ease with which data can be collected from Government-related websites. Core components of the Government's role are to ensure the nation's security and facilitate access to information. The assessment presented the issue of whether the national security process and in particular critical infrastructure protection can potentially be impeded by the availability of critical infrastructure data. More specifically, where the data collection process presented can be carried out more exhaustively by an individual's intent in compromising Australia's CI for various reasons such as vandalism, competitive intelligence, theft, fraud and terrorism.

While it is important to achieve a balance between open information access and data access restrictions/censorship in the interest of national security, this study highlighted the need to address the following questions in the Government arena: How much data should be provided to the public? Is it necessary that Government be completely open to the public in view of data provisioning? Should data be provided to community members based on their profile or need for the data? Should data be openly available to all citizens? Can data be categorised based on its sensitivity, and the appropriate restrictions be applied? Is public data availability and e-Government impeding the critical infrastructure protection process? What are the future steps for Government with respect to this situation?

6 Commercial data sources

Commercial data suppliers are bodies that provide products and/or services to their customers for a certain price, and under particular conditions. More importantly, they are involved in providing Government with data, which is ultimately purchased for internal Government and public use. The commercial bodies of interest to this study are those that provide information about critical infrastructure, and physical entities at a specific location. That is, they are involved in the provision of spatial data that can be represented on a map, with the associated geographic coordinates.

At the time of this study, the four major data supplying agencies of interest were MapData Sciences, PSMA, Sensis, and MapInfo. As was the case with the Government assessment, this selection of commercial suppliers is not complete, but rather was used to illustrate the commercial public data situation, and to provide an overview of the types of products and information that can be acquired.

It is significant at this point to reiterate the link between the Government and Commercial data sectors. Whilst data is available from the commercial bodies for a fee, Government agencies heavily rely on the Commercial sector for their data, and particularly mapping needs. Consequently, data and maps produced by Government are in some instances widely available for public access, use and distribution. This creates a situation where the link between the Government and Commercial data supplying agencies is becoming less defined (or blurred), and data is increasingly being made available to the extent that purchasing location-specific and CI-related data seems unnecessary, as free data is made available on the websites of Government Departments.

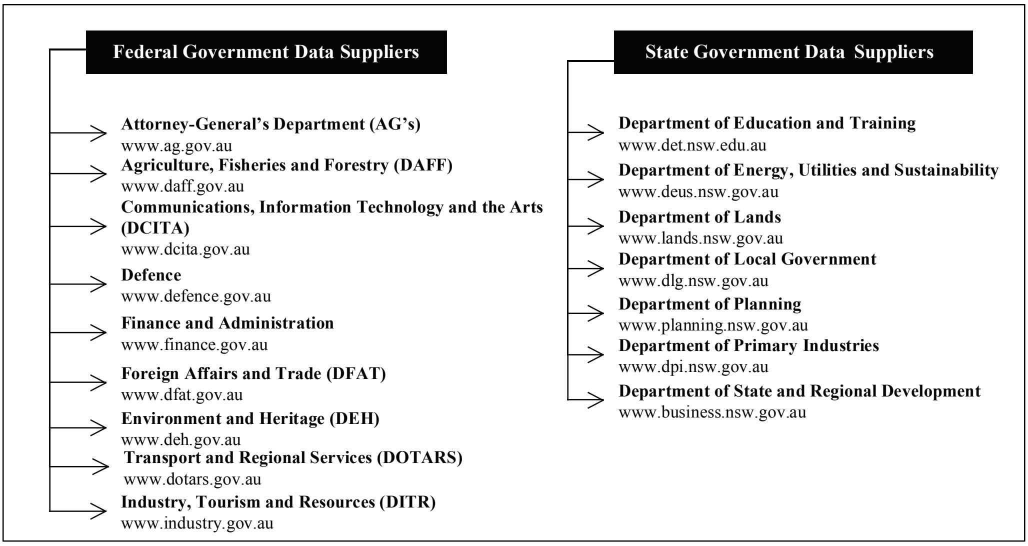

Federal Government Data Suppliers
Attorney-General's Department (AG's)
www.ag.gov.au
Agriculture, Fisheries and Forestry (DAFF)
www.daff.gov.au
Communications, Information Technology and the Arts (DCITA)
www.dcita.gov.au
Defence
www.defence.gov.au
Finance and Administration
www.finance.gov.au
Foreign Affairs and Trade (DFAT)
www.dfat.gov.au
Environment and Heritage (DEH)
www.deh.gov.au
Transport and Regional Services (DOTARS)
www.dotars.gov.au
Industry, Tourism and Resources (DITR)
www.industry.gov.au
State Government Data Suppliers
Department of Education and Training
www.det.nsw.edu.au
Department of Energy, Utilities and Sustainability
www.deus.nsw.gov.au
Department of Lands
www.lands.nsw.gov.au
Department of Local Government
www.dlg.nsw.gov.au
Department of Planning
www.planning.nsw.gov.au
Department of Primary Industries
www.dpi.nsw.gov.au
Department of State and Regional Development
www.business.nsw.gov.au

Figure 1 Federal and state government data supplying agencies

An additional crucial point is that any individual can access commercial data, provided that they have the necessary funds. With respect to an individual intent on causing harm, it is clear that no mechanisms screen the individual, and prohibit them from accessing the datasets. The motivation for suppliers in this category is evidently monetary; however the following questions must be posed: does gaining profit from the distribution of CI-related datasets justify compromising Australia's critical infrastructure, and introducing national security concerns? Additionally, should there be stringent mechanisms in place to manage the individuals accessing CI-related data to ensure that any risks are minimised?

7 Other data supplying agencies

Government and Commercially accessed data can further be supplemented with information from other sources, specifically the owners and operators of critical infrastructure items, such as utility and telecommunications companies. These bodies generally seek to educate the community about their products/ services, but are 'unintentionally' providing revealing information about their operations and infrastructure. Throughout this study, the major utility companies and telecommunications providers in Australia were assessed with respect to the amount of critical infrastructure data they offer.

Utility companies refer to organisations involved in providing energy (electricity and gas) and water-related services to the community. The major utility companies evaluated include Sydney Water, Hunter Water, Integral Energy, Energy Australia and AGL. The major telecommunications providers in Australia, Telstra and Optus, were also profiled in terms of their role in public data availability. As with the utility companies, telecommunications organisations provide public information solely for the role of educating the community, and promoting their services and networks.

However, the concerns previously raised, relating to national security and critical infrastructure protection are also applicable to this data supplier category. For instance, some agencies are making available information relating to energy networks in an attempt to be transparent with their customers, but are in turn creating a risk in providing such details, which can potentially comprise the CIP process.

8 The public data availability situation in Australia

The supplier identification and categorisation phase described above was employed primarily to assess the disparate sources of public data in Australia, in order to determine whether critical infrastructure data exists in the public domain. It is evident from the assessment that data can be provided deliberately or unintentionally, and can in both instances be reproduced. Data files, independently, may not appear particularly useful, but when stored with data from various other sources result in a structured repository of data relating to Australia's critical infrastructure, as was produced as part of this study (refer to Figure 2).

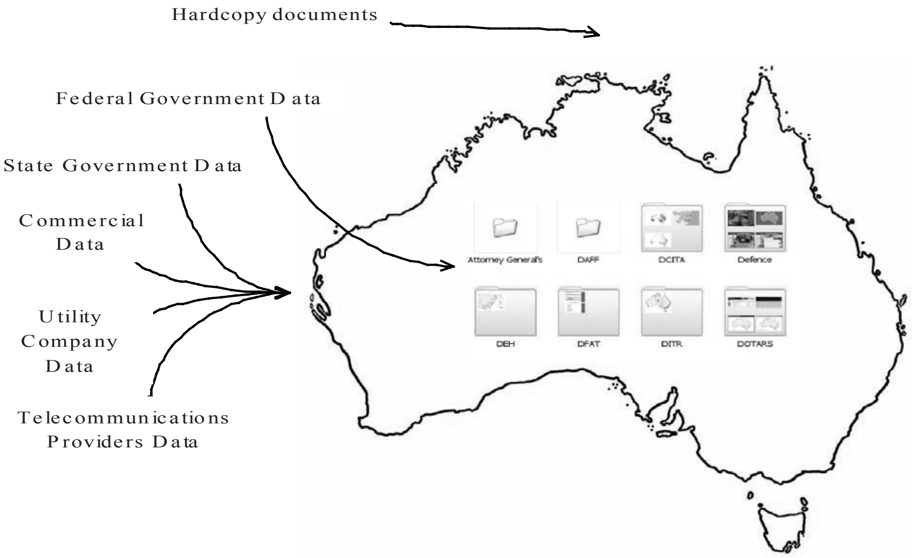


Figure 2 Australian critical infrastructure data repository

A repository of this nature allows for various characteristics of Australia's CI, both individual and collective, to emerge. Such characteristics include previously unconsidered patterns, interdependency information and vital data that may be revealing and compromise the CIP process, and thus affect national security. This structured process of collection can be replicated by any individual requiring little resources, and can be made more exhaustive and detailed with the appropriate funds and dedicated time. Therefore, an individual can engage in various preparations and activities with little inconvenience and detection, using publicly accessible information that was originally made available for the benefit of the public and to encourage openness in initiatives such as e-Government.

The data collected as a component of this study is essentially in its raw form; that is, no attempt has been made to manipulate the data and establish patterns or inferences for the purpose of creating scenarios and understanding the characteristics and linkages between infrastructure items. It is merely an initial repository of Australia's critical infrastructure-related data, collected from publicly available outlets. A selection of the data gathered from the identified bodies, the specific data elements, and the CI type(s) at risk is provided in Table 1.

In addition to the comparison in the table, the use of a geographic information system (GIS) can allow for the data elements to be further combined through the use of longitude and latitude coordinates, associating the data to a particular location. This allows for a graphical, map-based representation of CI-related data to be created, also allowing for detailed analysis of the data. Additional analysis and manipulation of the presented critical infrastructure data can also be conducted, to allow for more patterns and linkages to be revealed.

9 Conclusion

The outcome of this study is the identification of data supplying categories and agencies in Australia, and the creation of a data repository containing information relating to the country's critical infrastructure, by adapting the research conducted by Breeding (2003) in the United States. The examination highlighted the ease with which data could be collected, and the potential for more detailed gathering and analysis. It was apparent that a majority of the data has been provided for *positive* purposes; however, it appears that this level of transparency could result in negative implications for the CIP process. Furthermore, this assessment revealed that it is possible to simply engage in the creation of a comprehensive, sector-based repository of Australia's CI, with little detection or screening mechanisms. The Australian Government, through related Federal and State departments, offers a wealth of free data for public access. Other data supplying agencies are also present, such as commercial agencies, utility companies and telecommunications providers, who offer data both for profit and indirectly.

The data repository created, which was not exhaustive, demonstrated that revealing information can be publicly obtained in multiple formats, and can be stored for any purpose. While for research and emergency management activities this is important, a number of negative implications introduce the question of whether the positive uses of public data are overshadowed in certain situations. The potentially damaging effects of public data availability revolve around simplifying the ability to collect information that can compromise Australia's CI. These effects include terrorism, fraud, identity theft, vandalism, and competitive intelligence.

The ability to manipulate/present data in a form different from its original has demonstrated that 'sensitive but unclassified' data is in abundance in Australia. Data elements independently appear harmless, but techniques ranging in complexity and sophistication, such as geospatial information exploitation allow for inferences to be made and patterns to be extracted concerning Australia's CI, thus posing a threat to the CIP process.

The outcomes of this study were aligned with Breeding's, highlighting the potentially negative consequences enabled, and to an extent facilitated, by the provision of public data relating to Australia's CI. Further research into public data in Australia must be conducted, in an attempt to achieve a balance between open information access and restriction/censorship, to ensure that the threats associated with public data are minimised and eliminated where possible.

Table 1 Summary of public data and the threat to critical infrastructure

Supplier Type/Title	Major Available Data Elements (Attributes)	What CI is at Risk?
Federal/ Attorney General's Department	• Counter terrorism report & plan • Links to Emergency Management Australia & a set of publications/links	• All infrastructure types
Federal/ Agriculture, Fisheries & Forestry	• Food production & trade statistics	• Agriculture & the food supply
Federal/Communication Information Technology & the Arts	• Telephone services • Communications maps	• Communications • Cyber infrastructure
Federal/Defence	• Defence establishments • Video clips	• Government
Federal/Finance and Administration	• e-Government information	• Cyber infrastructure
Federal/ Foreign Affairs & Trade	• Trade statistics • Rail report • Rail network map • Supplier database	• Transport • All infrastructure types
Federal/Environment & Heritage	• Culture objects & places information • Power plant maps • Renewable energy	• Cultural icons • Energy
Federal/Transport & Regional Services	• 2006 transport statistics report • Transport map • Road, airport & rail network maps • Airline statistics • Shipping & ports statistics • Regional data	• Transport
Federal/ Industry, Tourism & Resources	• Energy supply details • Spreadsheet of renewable energy operators • Gas pipelines	• Energy
State/Department of Education & Training	• Searchable public school database • Statistical education information • Motorways in NSW (existing & proposed) • Freight & Rail infrastructure data	• Schools • Transport

Table 1 Summary of public data and the threat to critical infrastructure

Supplier Type/Title	Major Available Data Elements (Attributes)	What CI is at Risk?
State/Department of Energy, Utilities & Sustainability	• Local & metropolitan water utilities list • Sydney Water operations map • Energy Australia electricity network map • Gas network information • List of electricity suppliers	• Electricity • Gas • Water
State/Department of Lands	• Mapping tool for locating things such as roads, properties & national parks • Geographic names register CSV file	• All infrastructure types (particularly transport)
State/Department of Local Government	• Excel file of Council contact details • Detailed Council information by region • Councils map	• Government
State/Department of Planning	• Transport & population statistics, maps & graphs • Travel habits report	• Transport
State/Department of Primary Industries	• Map of mines • Petroleum, coal mines & energy maps & resources	• Energy
State/Department of State & Regional Development	• Economic, trade, infrastructure & business statistics & facts • Regional profile, with transport and major networks information • NSW train network • Ports data	• All infrastructure types (particularly transport)
Commercial/MapData Sciences	• Address locator • Street database, containing transport, towns & points of interest data	• All infrastructure types
Commercial/PSMA, G-NAF	• Points of interest, such as cultural, defence, emergency, medical, post offices, sewage, transport and utilities • Physical addresses datasets • Transport dataset	• All infrastructure types
Commercial/Sensis	• Telephone service • Business & residential information • Points of interest maps	• All infrastructure types
Commercial/MapInfo	• Streets, demographics, postal & administrative boundaries data	• All infrastructure types
Utility Companies/Sydney Water	• Area of operations map • Sewage treatment plants map • Water filtration & treatment plants information	• Water
Utility Companies/Hunter Water	• Supply & performance statistics • Dam fact sheets • Treatment plant diagrams • Area of operations map	• Water • Dams

Table 1 Summary of public data and the threat to critical infrastructure

Supplier Type/Title	Major Available Data Elements (Attributes)	What CI is at Risk?
Utility Companies/Integral Energy	• Network area maps	• Energy
Utility Companies/Energy Australia	• Network map • Proposed upgrades to electricity network map	• Energy • Electricity
Utility Companies/AGL	• Gas distribution network	• Gas
Telecommunications Providers/Telstra	• Network information • Interactive coverage maps	• Communications • Cyber infrastructure
Telecommunications Providers/Optus	• Network coverage maps • Broadband network map • Mobile coverage in NSW	• Communications

References

Australian Government (2006). 'About this Site' [Online]. Available: http://australia.gov.au/about-this-site [Accessed July, 2006].

Breeding, A. J. (2003). Sensitive but Unclassified Information: A Threat to Physical Security, SANS Institute [Online], Available: http://www.sans.org/rr/whitepapers/country/ [Accessed December, 2005].

Davey, S. (2005). 'Exploring e-democracy and Online Service Delivery for Australian Governments', CHISIG, Canberra, Australia, November 23-25.

Emergency Management Australia (2003). 'Mapping the Way Forward for Large-Scale Urban Disaster Management in Australia' [Online], Available: www.ema.gov.au [Accessed February, 2006].

Givens, B. (n.d.). 'Public Records on the Internet: The Privacy Dilemma' [Online], Available: www.privacyrights.org [Accessed March, 2006].

Lee, S. M., Tan, X. and Trimi, S. (2005). 'Current Practices of Leading e-government Countries', Communications of the ACM, 48(10): 99-104.

Luiijf, E. A. M. and Klaver, M. H. A (2004). Protecting a Nation's Critical Infrastructure: The First Steps. IEEE International Conference on Systems, Man and Cybernetics: 1185-1190.

Popp, R., Armour, T., Senator, T. and Nymrych, K. (2004). 'Countering Terrorism Through Information Technology', Communications of the ACM, 47(3): 36-43.

Punia, D. K. and Saxena, K. B. C. (2004). 'Managing Inter-organisational Workflows in eGovernment', Communications of the ACM: 500-505.

Wunnava, S.V and Reddy, M.V. (2000). 'Internet Based Digital Government Model Development', Florida International University College of Engineering, IEEE 2000: 205-208.

18

Privacy and national identity cards: A legal and technical study

Steven R Clark

PhD Candidate, Centre for Regulation and Market Analysis, University of South Australia

Abstract

This paper outline a work-in-progress, part of a larger research project with respect to the alignment of legal and technical privacy protection measures in government identity management systems. The recent history of attempts to introduce national identity cards in Australia is summarised. This provides context for a brief discussion of privacy research regarding pervasive technologies such as universal identity cards. Privacy concerns often centre upon the surveillance potential of identity technologies. Here an alternative model for conceptualising privacy is presented, to further inform the development of a framework for integrating legal and technological mechanisms for managing privacy in information management systems.

Keywords: privacy, law, identity cards, pervasive technologies, information privacy, information security.

1 Introduction

> To the extent that the individual has no control over, and perhaps no knowledge about, the mass of identifiable data which may be accumulated concerning him or her, and to the extent that national law-makers, despite their best endeavours, enjoy only limited power effectively to protect the individual in the global web, privacy as a human right, is steadily undermined (Kirby 1998).

Serious public debate regarding a national identity card is long overdue (Davies 2005; Greenleaf 2007e). This paper describes part of a doctoral research project that will investigate the legal and technological measures intended to protect the privacy and integrity of personal data held in government identification management systems in Australian and British contexts. This larger research project will begin with a re-examination of the most recent attempts to introduce a nation-wide, integrated government identity management system.

Contemporary information systems typically involve information being acquired, stored, processed and shared by and between internal and external entities. A crucial component of these systems is the identification and authentication of individuals to the system. Once a person has been authenticated to the system, appropriate authorities and services can then be allocated.

Adequate identification and authentication of users and subjects within information systems can raise a range of privacy and security issues (Camp 2003; 6 2005; Weis 2005; Sullivan 2006; Zalud 2006). These concerns become particularly acute when the desires of a State (and its citizens and residents) to protect the security and integrity of the State conflicts with the desire of those same citizens and residents to have their privacy respected and protected by the State. Finding adequate resolutions to those conflicts is rarely straightforward (6 2005; Kirk & Bucken 2006; Udell 2006; Zalud 2006).

Identification technologies afford significant convenience when dealing with bureaucracies and complex information systems. But they do not have an uncontroversial history. Technologies that deal with personal information can raise the spectre of Orwellian Big Brother governments and Kafkaesque bureaucracies. Fears that technologies might slip beyond our capacity to regulate and control – metamorphosing to regulate and control us instead – are by no means new.[1] Of particular concern are technologies that can be used to identify, trace, and/or track individuals or groups.

At the same time, increasing familiarity and comfort with these technologies (at least, with the convenience they offer) leads to their increasing normalisation and invisibility. The implications of this trend on the social and legal interests of those who do (and do not) adopt them is of significant interest and importance (Bohn

[1] History offers up sabotage, the Luddites, and significant portions of science fiction – including George Orwell's iconic *Nineteen Eighty-four* – as examples.

et al. 2005; Coroama et al. 2005).

This research will consider relevant legal issues (Iachello & Abowd 2005; Herskovic, Ochoa & Pino 2006; Subirana & Bain 2006; Ciocchetti 2007) and related socio-technological design issues (Bellotti & Sellen 1993; Langheinrich 2001; Seigneur & Jensen 2004; Lahlou, Langheinrich & Röcker 2005; Sacramento, Endler & Nascimento 2005; Ciocchetti 2007) raised by technologies in the context of trusted forms of identification.

It is anticipated that this research will be of interest to policy makers, government agencies, private organisations, academics, and individuals and groups. It is also intended to foster and contribute to a wider community dialogue regarding the introduction of government-sponsored identity cards (6 2005; Deane 2005; 2005; Jackson & Ligertwood 2006; Greenleaf 2007a; Whitley et al. 2007).

2 History

Prior to 1985, identity cards had not been on the Australian political landscape since the end of the Second World War, some forty years earlier (Greenleaf & Nolan 1986). The seven year review of privacy issues, between 1975 and 1983, by the Australian Law Reform Commission found no need to discuss identity cards (Australian Law Reform Commission 1983).

2.1 The Australia Card

In June 1985, at a National Taxation Summit, the then Federal Minister for Health unveiled a bold new proposal: the 'Australia Card'. This was to be an ambitious program centred on a national identity card linked to a computer register to enable Government agencies to monitor, amongst other things, taxation and other financial transactions (Greenleaf & Nolan 1986).

Within a year the proposal had been the subject of a White Paper, two Inter-Departmental Committees comprising a dozen Federal departments, several ALP Caucus deliberations, the Tax Summit, and a Joint Select Committee of the Federal Parliament. Commentators at the time criticised the process and the proposal for being rushed and ostensibly driven by bureaucracy for its own purposes (Greenleaf & Nolan 1986).

The Australia Card was to have seven key elements: (Greenleaf & Nolan 1986)

- a universal, compulsory identity card (the Australia Card),
- a unique identification number (UIN) for every individual,
- a central computer register (Australia card register, ACR) for 'basic identifying details',
- a national births, deaths and marriages (BD&M) register,
- an online telecommunications network linking agencies with the central register,
- a 'companion entity system' matching corporate and unincorporated entities to the system through the UIN of an identified 'relevant person', and

- a new agency, the Data Protection Agency (DPA) to supervise the use of the system by the ATO, DSS and HIC (but *not* everyone else).

The program initially garnered widespread support, but flaws in the enabling legislation intensified privacy concerns (Greenleaf 2007e, p 34) and other issues. The Australia Card proposal ultimately failed because public opinion swung against it during the 18 months between its announcement and eventual withdrawal.

2.2 The Access Card system

Twenty years later, a Liberal government was proposing a similar system. The Health and Social Security Access Card (Access Card) system was to be one of the most significant information technology implementations in Australian society. Within two years of the system's implementation almost every adult resident in Australia was to have had a card. Without it, no one could draw upon their legal entitlement to government health and welfare benefits (Hockey 2006). A child's access was to be mediated through their legal guardian/parent's card.

If this were not significant enough, the government's proposal extended the scope of the system into general commercial transactions through a section of the card intended to be accessible by third parties with the card holder's/owner's 'consent' (Hockey 2006).

2.3 Comparing the Australia Card and Access Card proposals

A number of features in the Access Card proposal took advantage of developments in technology, and perhaps also social context. There was significantly less public debate around the implications and functions of the Access Card than there had been regarding the Australia Card. Concerns and objections raised were at least in part about *how* such a system is implemented and regulated.

The Howard Government strenuously denied that the Access Card was, or would ever be, a national identity card. In contrast, the Australia Card was intended to be a national identity card. But there are significant similarities between the two (Greenleaf 2007e). History suggests that the Access Card was likely to become a *de facto* national identity card. For example, drivers' licences are not intended to be identity documents beyond evidence of a licence to drive, but they are regularly used and accepted as such. Indeed, they are included in the Commonwealth Government's Proof of Identity Points Scheme for use by banks, etc (Hockey 2006).

Both cards would have effectively been compulsory and practically universal amongst adults. Carrying the Access Card would not have been compulsory, and only required for specified transactions. Crucially, the Access Card's Secure Customer Registration System (SCRS) would confirm *current* eligibility for concessions by pharmacists and medical practitioners. The Australia Card legislation included limits, though flawed, on the potential uses of the card. This was less clear in the Access Card proposal (Greenleaf 2007e, p 35).

On their face, the two cards do not appear to be much different. The details to be printed on the cards were essentially the same. However, the Australia Card was to be a swipe card of the type in use by banks and the Medicare card. The magnetic stripe on the back of the card had limited data storage capacity. The Access Card 'smartcard', in contrast, contains a microchip enabling significantly more data to be carried, and the potential for a much broader range of functions. Indeed, the Access Card was intended to have an 'electronic purse' function, with emergency welfare payments to be stored on the card itself (Greenleaf 2007e, p 35).

The computer system that the card is designed to interface with is at least as important as the card itself. Both systems relied upon a central register database. The Australia Card Register (ACR) was far more limited in scope than the proposed Secure Customer Registration System (SCRS). The ACR was to contain little more than identification data and a current address (Greenleaf 2007e, p 35).

The SCRS was to have held copies of all identification documents provided at registration, plus a photograph and other details regarding the registrant. This would have made it the first and 'only comprehensive photographic database of Australians'(Greenleaf 2007e, p 35). It would therefore be possible to cross-match other photographic and video records against the database, for example to identify people in CCTV footage or to scan crowds for particular individuals. While this was not actually proposed (Greenleaf 2007e, p 35), it would be of significant interest to law enforcement and security agencies – public and private (Sarre & Prenzler 2005).

2.4 Tax File Number instead

When the Australia Card proposal failed, the government of the time compromised by introducing a card-less identifier with far more limited uses and without a central register: the Tax File Number (TFN) (Greenleaf 2007e, p 34). Nevertheless, within two years the Keating Government had expanded that system to enable data matching of social welfare systems against TFN records (Greenleaf 2007e, p 34). Scope creep is an enduring issue with computerised systems.

2.5 Public debate regarding identity card privacy issues

That a universal identifier or identification token would impose unacceptable risks to individual privacy was a significant concern in the literature and in public debate (Greenleaf 2007e). It has been argued, for example, that the biometrics proposed for the Access Card are unacceptable – but similar biometrics are used in Australian passports already (Department of Foreign Affairs and Trade 2008).

The rejection of the Australia Card in 1987 has entrenched a view that a National Identity Card can *never* be acceptable in Australia. Following the announcement of the Access Card proposal, public discussion focused upon the privacy implications of the system for individuals (Greenleaf 2007a, b, c, d, e). Other concerns raised included the cost to implement and maintain the system and other practicalities. These are by no means new, nor limited to Australia (Davies 2005).

3 Privacy and identity card technologies

A significant trend in the development of computer-based technologies is its increasing pervasiveness. Computers of one kind or another can be found everywhere, and in almost everything – particularly in contemporary technologically 'advanced' societies. This trend to embed computers into the fabric of our society has been called 'ubiquitous computing', 'pervasive computing', 'calm technology', 'things that think', and 'everyware' (Greenfield 2006). A universal identity management system (such as a national identity card or a national health services card) that mediates access to government-provided and government-funded services would certainly become pervasive, even if it were not designed to be so from the outset.

The privacy implications of pervasive technologies have attracted significant research interest (Bellotti & Sellen 1993; Langheinrich 2001, 2002a; Davies 2005; Dourish & Anderson 2005; Floerkemeier, Schneider & Langheinrich 2005; Langheinrich 2005, 2007; Speicys Cardoso & Issarny 2007). Computer technologies have raised privacy concerns in Australia (Greenleaf 2007a) and elsewhere (Taskforce on Privacy and Computers 1972; Murakami 2004; Davies 2005) since the earliest days. The impact of technologies upon the privacy of both the community and individuals (Luong 2006; March & Fleuriot 2006) is an enduring source of lively debate.

Debates surrounding security have often been in conflict with concerns about privacy. To be effective, privacy and security mechanisms have to be designed into technology (Langheinrich 2001, 2002a, b; Dourish & Anderson 2005; Floerkemeier, Schneider & Langheinrich 2005; Langheinrich 2005; Langheinrich et al. 2005; Langheinrich 2007). Design must reflect actual, real, and effective controls. Security in the realm of pervasive technologies has placed significant emphasis on controlling access (through physical and logical barriers) and on trust and trustworthiness (Bohn et al. 2004; Ranganathan 2004; Weis 2005).

Wide-spread use of pervasive technologies has the potential to enable significant invasions of privacy.[2] Protection against these risks could come from one or more of the following approaches: legislation, codes of practice, new technologies and, less probably, informed choice on the part of the user (Anders & Hansson 2003; Price, Adam & Nuseibeh 2005).

Since the collection of information via pervasive technologies can enable observation almost anywhere and everywhere, there is the potential for a perception of 'pervasive observation' (ala Orwell's Big Brother) (Bohn et al. 2004; Schmandt & Ackerman 2004; Olson, Grannis & Mandl 2006). Examples include fears that every public CCTV camera[3] might be cross-matched with identity databases, or that GPS-

[2] For example, data mining techniques can easily be applied to data from multiple data sources to build a composite picture of an individual. Furthermore, the source data or composite picture may be the subject of accidental or malicious alteration.

[3] London is an example of a city where CCTV cameras are practically ubiquitous: more than ten thousand publically-owned cameras alone.

enabled mobile phones could be used to track the movements of users (Schmandt & Ackerman 2004; Lahlou, Langheinrich & Röcker 2005). Careful consideration of the distinct privacy and security dimensions of these concerns can illuminate not only their origins, but may also suggest appropriate responses (Langheinrich 2001, 2005).

4 Privacy laws and identity cards

Legal culture has a direct effect on the implementation of identity card systems (Davies 2005). The collection, handling and storage of data are central to such systems. These processes raise security and privacy concerns regarding the management of the data. Laws are traditionally used to regulate behaviour and technologies, and penalise for non-compliance. Many countries have privacy laws to define and protect the appropriate gathering, storage and uses of information.

Privacy has proven very difficult to explain or define to everyone's satisfaction. The 'classic' legal definition of privacy, 'the right to be let alone' (Warren & Brandeis 1890, p 195), has been criticised by many commentators for failing to adequately encompass the social dimensions of the concept. Nevertheless, this inability to clearly define 'privacy' has not prevented some notion of privacy holding sway in the community.

The concept of privacy is considered so important, and so widespread, that it has been recognised as an international legal norm. For example, Article 12 of the Universal Declaration of Human Rights (UDHR) (and the practically identical Article 17 of the International Covenant on Civil and Political Rights (ICCPR)) says:

> 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 (United Nations General Assembly 1948, 1966).

These norms influence national laws in a variety of ways; dependant upon pre-existing laws, social norms, and legal culture.

Privacy laws in Australia are largely limited to addressing information privacy[4] (Clarke 2008). The main information privacy mechanism is the federal *Privacy Act 1988* (Cth) which regulates Commonwealth government agencies, and corporations and healthcare entities. The Act sets out Information Privacy Principles (IPPs) for Commonwealth and ACT government agencies and National Privacy Principles (NPPs) for corporations and health service providers. The Act also regulates credit providers and credit reporting agencies. There are other relevant federal, state and territory laws.

[4] Roger Clarke defines 'information privacy' as 'the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.' Clarke, R 2006, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, updated 7 August 2006, viewed 3 July 2008, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

Any national identity card system would have to comply with a plethora of privacy regulations and legislation. The Australian Law Reform Commission is currently undertaking a comprehensive review of privacy laws. The complexity and diversity of existing laws are part of the remit. A Discussion Paper (Australian Law Reform Commission 2007) has been released, outlining proposals for greater consistency within the *Privacy Act 1988* (Cth) and uniformity across Australian jurisdictions. The Final Report is expected sometime after 31 March 2008.

5 Metaphors for privacy concerns

The right metaphor can assist in developing good legal and technical solutions by helping to capture the essence of a problem. Solove suggests that much of the debate surrounding privacy is about the kind of society we want to be living in – it's 'feel and atmosphere'. Literary metaphors are good at capturing moods, and can 'effect[sic] the way we see a problem and the way we solve a problem'(Caplan 2001).

Identity cards are often portrayed as quintessential devices in the apparatus of the totalitarian state. Cross-matching thousands and millions of records in moments, collecting and collating incredibly detailed records regarding individuals and their use of such cards, affords enormous scope for surveillance. Individuals can be excluded from the system to achieve power over them, or included in it and thereby perhaps empowered in otherwise faceless bureaucracies.

5.1 Big Brother surveillance

In the English-speaking West, there is a widely-held fear of Big Brother – the idea of a State or its apparatus exercising ubiquitous and pervasive surveillance power to control individuals (Orwell 1949). Sections of our community rail against any and all moves to increase or extend government authority without adequate oversight and accountability (Hockey 2006). These are laudable efforts, but of increasing concern are the many Little Brothers – corporate and private entities – that have access to and/or maintain control over significant collections of personal information for their (commercial) benefit (Sarre & Prenzler 2005).

Private entities have been gaining increasing access to government-collected, government-held information. Outsourcing, privatisation and other commercial arrangements have changed the relationships between government and private entities over many years. Not only are private entities privy to more and more government information, they are increasingly responsible for collecting and processing as well. In Australia, the rules governing the collection, storage, processing and uses of personal information often differ between government and private entities (Sarre & Prenzler 2005).

5.2 Kafkaesque bureaucracy

Solove has proposed an alternative literary metaphor for privacy issues in a digital society (Solove 2001). In *Nineteen Eighty-Four*, George Orwell's Big Brother personifies a ubiquitous totalitarian surveillance state that monitors everything you say and do. This produces an environment of 'dreary conformity' where fear leads to self-censorship. Solove suggested that Kafka's *The Trial* might offer a more appropriate metaphor for privacy issues (Caplan 2001; Solove 2001). Jack Balkin[5], suggests that while Orwell envisages an evil, brooding entity actively working against you, Kafka has you 'trapped in a maze'(Caplan 2001).

In Kafka's *The Trial*, Joseph K wakes up one morning to find a group of government officials in his apartment. They tell him he is under arrest, but instead of detaining him, they leave. An absurd odyssey follows as Joseph is unable to find out why he is under arrest, or intervene in his own trial. The Court is secret and refuses to reveal what information they have or who is trying him. At the end of the book, he is seized and executed (Caplan 2001).

The Trial is filled with impotence, anxiety and anger as an unseen bureaucracy uses information that Joseph has no access to or control over. Solove suggests this is similar to the loss of privacy many feel when dealing with computer databases. We are not heading towards a society of Big Brother or Little Brothers, rather one of arbitrariness, indifference and dehumanisation (Solove 2001).

While surveillance laws are important to constrain the acquisition and disclosure of confidential information, more of the same does not help. Solove argues that understanding privacy as a surveillance issue doesn't adequately account for why collecting information that is neither embarrassing nor significant of itself can be a problem. Privacy can be invaded without revealing secrets and without active observation (Solove 2001).

Solove argues that better regulation of what information may be collected and processed, and how it is to be stored and used *into the future* – limiting its propagation between databases. Providing accountability mechanisms, and making systems more transparent and accessible to clients and data subjects, shifts the balance of power towards the client and data subject. Solove suggests this will go a long way towards 'easing the average person's dreadful sense that he [or she] has little or no control over [her or] his personal information.' (Caplan 2001)

6 Informing a legal framework for identity card privacy

This research will be a component of a PhD examining the legal and technological issues surrounding the privacy and integrity of personal data obtained and held by Australian and British governments in identity management systems. One objective of the research is to inform and engage in a public discussion of identity card systems in an Australian context (Davies 2005; Greenleaf 2007e). While the current Australian government has dismissed a national identity card for the time being (Dearne 2008), they are unlikely to fall off the agenda entirely (Quade 1983; Ware 1986; Cassidy 1995; Benson 2002; Davies 2005; Harper 2006; Loller 2007; MacLean 2007; Overton 2007; Whitley et al. 2007).

[5] Knight Professor of Constitutional Law and the First Amendment at Yale University.

7 Conclusion

Privacy is an enduring concern in society. In recent debates, privacy has often been cast at odds with security. As technologies and systems are designed and implemented to deliver more convenient access to government services, they are also enabling more extensive and invasive inroads into previously private parts of our lives. Individuals, government agencies, and service providers all have legitimate interests in the integrity and privacy of data and information held in identity management systems used to mediate access to those services.

When privacy and security have come into conflict, technologies have tended to favour security at the expense of privacy. Since privacy is still an important – and hotly contested – value in our society, a more holistic approach is needed to identify and balance the competing interests in these three issues.This research aims to produce a framework for integrating legal and technological mechanisms towards that objective.

References

6, P 2005,'Should We Be Compelled to Have Identity Cards? Justifications for the Legal Enforcement of Obligations', *Political Studies,* vol. 53, no. 2, 06, pp. 243-261.

Anders, JP & Hansson, SO 2003,'Privacy at Work - Ethical Criteria', *Journal of Business Ethics,* vol. 42, no. 1, pp. 59-70.

Australian Law Reform Commission 1983, *Privacy, Report 22*, Australian Law Reform Commission, Canberra.

Australian Law Reform Commission 2007, *Review of Australian Privacy Laws, Discussion Paper 72*, Australian Law Reform Commission, Sydney, NSW.

Bellotti, V & Sellen, A 1993, *Design for Privacy in Ubiquitous Computing Environments*, Rank Xerox EuroPARC, Cambridge, UK.

Bennett Moses, L 2007,'Recurring Dilemmas: The Law's Race to Keep Up With Technological Change', *University of New South Wales Faculty of Law Research Series*, no. Working Paper 21, April

Benson, M 2002,'Nationwide ID-card system remains chilling prospect.(Editorial)', *The Los Angeles Daily Journal*, p. 6, <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A94457660&source=gale&srcprod=LT&userGroupName=unisa&version=1.0 >.

Bohn, J, Coroama, V, Langheinrich, M, Mattern, F & Rohs, M 2004,'Living in a World of Smart Everyday Objects - Social, Economic, and Ethical Implications', *Journal of Human and Ecological Risk Assessment,* vol. 10, no. 5, pp. 763-785.

Bohn, J, Coroama, V, Langheinrich, M, Mattern, F & Rohs, M 2005,'Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing', in *Ambient Intelligence*, eds. Weber, W, Rabaey, J & Aarts, E, Springer-Verlag, pp. 5-29.

Camp, LJ 2003,'Identity, authentication, and identifiers in digital government', paper presented at the International Symposium on Technology and Society, 2003/Crime Prevention, Security and Design, 2003.

Caplan, CS 2001, *Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy*, The New York Times.

Cassidy, P 1995, 'Proposed national ID card threatens civil liberties', *The Los Angeles Daily Journal*, p. p6, <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A16048271&source=gale&srcprod=LT&userGroupName=unisa&version=1.0 >.

Ciocchetti, CA 2007, 'E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors', *American Business Law Journal,* vol. 44, no. 1, Spring, pp. 55-126.

Clarke, R 2006, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, updated 7 August 2006, viewed 3 July 2008, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>.

Clarke, R 2008, *Roger Clarke's Dataveillance and Information Privacy Home-Page*, viewed 3-4 July 2008, <http://www.anu.edu.au/people/Roger.Clarke/DV/>.

Coroama, V, Kostakos, V, Magerkurth, C & Vallejo, ILd 2005, 'UbiSoc 2005: first international workshop on social implications of ubiquitous computing', paper presented at the CHI '05 extended abstracts on Human factors in computing systems, Portland, OR, USA.

Davies, S 2005, 'The Complete ID Primer', *Index on Censorship,* vol. 34, no. 3, pp. 38-43.

Deane, A 2005, 'Identity Cards in Britain', *Contemporary Review,* vol. 286, no. 1672, May, pp. 268-270.

Dearne, K 2008, 'Smart cards off Labor agenda', *The Australian*, June 11, <http://www.australianit.news.com.au/story/0,24897,23847150-5013044,00.html>.

Department of Foreign Affairs and Trade 2008, *The Australian ePassport*, DFAT, Canberra ACT, viewed 6 May 2008, <http://www.dfat.gov.au/dept/passports/>.

Dourish, P & Anderson, K 2005, 'Privacy, Security ... and Risk and Danger and Secrecy and Trust and Morality and Identity and Power: Understanding Collective Information Practices', *ISR Technical Report*, no. UCI-ISR-05-1, January, pp. 1-19.

Floerkemeier, C, Schneider, R & Langheinrich, M 2005, 'Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols', paper presented at the Second International Symposium on Ubiquitous Computing Systems, UCS 2004, Tokyo, Japan, November 8-9, 2004.

Greenfield, A 2006, *Everyware: the dawning age of ubiquitous computing*, New Riders, Berkeley, CA.

Greenleaf, G 2007a, *'Access All Areas': Function Creep Guaranteed in Australia's ID Card Bill (No. 1)*, University of New South Wales - Faculty of Law.

Greenleaf, G 2007b, ''Access all areas': Function creep guaranteed in Australia's ID Card Bill (No. 1)', *Computer Law & Security Report,* vol. 23, no. 4, pp. 332-341.

Greenleaf, G 2007c, 'Asia-Pacific Developments in Information Privacy Law and its Interpretation', *University of New South Wales Faculty of Law Research Series* vol. Working Paper 5, January

Greenleaf, G 2007d, 'Australia's proposed ID card: Still quacking like a duck', *Computer Law & Security Report,* vol. 23, no. 2, pp. 156-166.

Greenleaf, G 2007e, 'The proposed 'access card': why we need a national id card debate', *Precedent,* vol. 78, pp. 34-38.

Greenleaf, G & Nolan, J 1986, 'The Deceptive History of the 'Australia Card'', *Australian Quarterly,* vol. 58, no. 4, pp. 407-425.

Harper, J 2006, 'A national ID card?' *Chicago Daily Law Bulletin*, p. 5(1), <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A150391428&source=gale&srcprod=LT&userGroupName=unisa&version=1.0 >.

Herskovic, V, Ochoa, SF & Pino, JA 2006, 'A Model to Incorporate Privacy in Organizational Memory Systems', paper presented at the 10th International Conference on Computer Supported Cooperative Work in Design, May 2006.

Hockey, J 2006, 'Future Directions for the Access Card: Your Card – Your Security', paper presented at the National Press Club, Canberra, 8 November.

Iachello, G & Abowd, GD 2005, 'Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing', paper presented at the Conference on Human Factors in Computing Systems: Technology, Safety, Community (CHI '05), Portland, OR.

Jackson, M & Ligertwood, J 2006, 'Identity Management: Is an Identity Card the Solution for Australia?' *Prometheus,* vol. 24, no. 4, 12, pp. 379-387.

Kirby, M 1998, 'Privacy in Cyberspace', *University of New South Wales Law Journal,* vol. 21, pp. 325-326.

Kirk, J & Bucken, M 2006, 'British Lawmakers Question ID Card Plan', *Computerworld,* vol. 40, no. 4, 01/23/, pp. 16-16.

Lahlou, S, Langheinrich, M & Röcker, C 2005, 'Privacy and trust issues with invisible computers', *Communications of the ACM,* vol. 48, no. 3, pp. 59-60.

Langheinrich, M 2001, 'Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems', paper presented at the Third International Conference on Ubiquitous Computing (UbiComp 2001), Atlanta, USA.

Langheinrich, M 2002a, 'A Privacy Awareness System for Ubiquitous Computing Environments', paper presented at the 4th International Conference on Ubiquitous Computing (Ubicomp 2002), September.

Langheinrich, M 2002b, 'Privacy Invasions in Ubiquitous Computing', paper presented at the Ubicomp Privacy Workshop, Gteborg, Sweden.

Langheinrich, M 2005, 'Personal Privacy in Ubiquitous Computing - Tools and System Support', PhD thesis, ETH Zurich.

Langheinrich, M 2007, 'RFID and Privacy', in *Security, Privacy, and Trust in Modern Data Management*, ed. Jonker, W, Springer, Berlin Heidelberg New York.

Langheinrich, M, Coroama, V, Bohn, J & Mattern, F 2005, 'Living in a Smart Environment - Implications for the Coming Ubiquitous Information Society', *Telecommunications Review,* vol. 15, no. 1, February, pp. 132-143.

Loller, T 2007, 'Some immigrants can't marry for lack of social security card', *Chicago Daily Law Bulletin*, p. 1(2), <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A166835174&source=gale&srcprod=LT&userGroupName=unisa&version=1.0 >.

Luong, K 2006, 'The other side of identity theft: not just a financial concern', paper presented at the 3rd Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia.

MacLean, PA 2007, 'Push for standard ID riles states', *The National Law Journal*, p. NA, <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A163328147&source=gale&srcprod=LT&userGroupName=unisa&version=1.0>.

March, W & Fleuriot, C 2006, 'Girls, technology and privacy: "is my mother listening?"', paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Montréal, Québec, Canada.

Murakami, Y 2004, 'Privacy issues in the ubiquitous information society and law in Japan', paper presented at the IEEE International Conference on Systems, Man and Cybernetics, 2004.

New York Times 2005, 'An Unrealistic 'Real ID'', *New York Times*, May 4, p. A22, <http://ezlibproxy.unisa.edu.au/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=17102962&site=ehost-live >.

Olson, KL, Grannis, SJ & Mandl, KD 2006, 'Privacy Protection Versus Cluster Detection in Spatial Epidemiology', *American Journal of Public Health,* vol. 96, no. 11, 11, pp. 2002-2008.

Orwell, G 1949, *Nineteen eighty-four: a novel*, Secker & Warburg, London.

Overton, S 2007, 'Voter identification', *Michigan Law Review,* vol. 105, no. 4, p. 631(51).

Price, BA, Adam, K & Nuseibeh, B 2005, 'Keeping ubiquitous computing to yourself: A practical model for user control of privacy', *International Journal of Human Computer Studies,* vol. 63, no. 1-2, pp. 228-253.

Quade, V 1983, 'ID card for all? Alien-tracing plan under fire', *ABA Journal,* vol. 69, pp. 1370-1371.

Ranganathan, K 2004, 'Trustworthy pervasive computing: The hard security problems', paper presented at the Second IEEE Annual Conference on Pervasive Computing and Communications (PerCom 2004), Orlando, FL.

Sacramento, V, Endler, M & Nascimento, FN 2005, 'A Privacy Service for Context-aware Mobile Computing', paper presented at the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.

Sarre, R & Prenzler, T 2005, *The Law of Private Security in Australia*, Lawbook Co,

Schmandt, C & Ackerman, M 2004, 'Personal and Ubiquitous Computing: Issue on privacy and security', *Personal Ubiquitous Computing,* vol. 8, no. 6, pp. 389-390.

Seigneur, J-M & Jensen, CD 2004, 'Trust enhanced ubiquitous payment without too much privacy loss', paper presented at the 2004 ACM Symposium on Applied Computing, Nicosia, Cyprus.

Solove, DJ 2001, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review,* vol. 53.

Speicys Cardoso, R & Issarny, V 2007, 'Architecting Pervasive Computing Systems for Privacy: A Survey', paper presented at the Working IEEE/IFIP Conference on Software Architecture, 2007 (WICSA '07), Mumbai, India.

Subirana, B & Bain, M 2006, 'Legal Programming', *Communications of the ACM,* vol. 49, no. 9, 09, pp. 57-62.

Sullivan, RK 2006, 'The Authentication Imperative', *U.S. Banker,* vol. 116, no. 6, June, p. 46.

Taskforce on Privacy and Computers 1972, *Privacy & Computers*, Department of Communications & Department of Justice, Ottawa, Canada.

Udell, J 2006, 'National Identities', *InfoWorld,* vol. 28, no. 40, 10/02/2006, p. 30.

United Nations General Assembly 1948, *Universal Declaration of Human Rights (UDHR)*, Palais de Chaillot, Paris.

United Nations General Assembly 1966, *International Covenant on Civil and Political Rights*.

Ware, D 1986, 'The Australia card program', *Legal Service Bulletin*, pp. 198-201, <http://find.galegroup.com/itx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T004&prodId=LT&docId=A4661623&source=gale&srcprod=LT&userGroupName=unisa&version=1.0>.

Warren, SD & Brandeis, LD 1890, 'The Right to Privacy', *Harvard Law Review,* vol. 4, no. 5, December 15, pp. 193-220.

Weis, SA 2005, 'Security parallels Between People and Pervasive Devices', paper presented at the 3rd International Conference on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops).

Whitley, EA, Hosein, IR, Angell, IO & Davies, S 2007, 'Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme', *The Information Society,* vol. 23, pp. 51-58.

Zalud, B 2006, 'Privacy and IDs', *Security: For Buyers of Products, Systems & Services,* vol. 43, no. 12, December 2006, p. 60.

19

Using a RFID-University-based laboratory for homeland security applications testing

Samuel Fosso Wamba

Lecturer, School of Information Systems and Technology, University of Wollongong
Academic Founder of Academia RFID

Abstract

Radio-frequency identification (RFID) technology is emerging as one of the most pervasive computing technologies capable of enabling the Mark Weiser vision of ubiquitous computing where technology is seamlessly incorporated into our daily lives (Weiser, 1991; Roberts, 2006). The technology has attracted considerable interest from businesses, academics and governments in recent years. The interest is even stronger in some countries such as Canada and USA where policy makers are exploring the potential of the technology to enhance homeland security applications such as e-Passport and Customs-Trade Partnership against Terrorism (C-TPAT). This paper provides some insights into a RFID-University-based laboratory that acts as a pole of innovation for homeland security applications testing and shows through a case study how the laboratory helps Canadian small-to-medium enterprise (SME) to fulfil the C-TPAT.

Keywords: RFID technology, laboratory, homeland security, testing, SMEs

References

Roberts, CM 2006, 'Radio Frequency Identification (RFID)', Computers & Security, 2006, vol. 25, no. 1, pp. 18-26.

Weiser, M 1991, 'The computer of the 21st century', Scientific American, pp. 94–100.

20

Biometric data management: Challenges, policies and best practices

Suzanne Lockhart

Chief Executive Officer, Biometric Consulting Group

Abstract

For leaders in the public sector the emerging debate over enhancing identity management systems utilising biometric technology will be amongst the most important of all matters to shape the coming information age. Competing policy interests range from protecting citizens freedoms, privacy and other prerogatives on one end of the scale to ensuring law and order, national security and institutional efficiencies on the other end. The challenge of implementing biometric systems is ensuring it provides functionality across all stages whilst taking into account the policy, procedures and best practices to support the proper management and administration of biometric data. An integral component is therefore constructing a framework for identity management where these and other issues can be addressed, best practices established and high-level standards developed. This paper will highlight and discuss some of the significant and challenging policy, procedural, social, legal and technological issues associated with supporting the proper management and administration of biometric data in large-scale centralised systems.

Keywords: biometrics, identity, data management, policies, best practices, law, social implications, citizens, centralised systems

21

What is trust online?

Nigel Phair

Principal eSecurity Consulting

Abstract

The online environment is just like the real world. When using the internet, people should use their real world sensibilities, just as you would with everyday social and economic transactions. Societal norms dictate that internet users operate ethically and lawfully.

Whether online or offline there are several factors which come into play: how and where you are interacting with a person; the nature of the transaction (you need more trust for a financial transaction than a chat); and the other parties reputation. The simple fact is that online, the majority of internet users (consumers, businesses, etc) don't know who they are interacting with. It is also well known that identity theft can be easily done in the online world, just as it is in the real world. The credentials we rely on to 'identify' someone (currently the 100 points system) is pretty much worthless.

Keywords: Trust, credentials, identity, social networking

1 What is identity?

To most people, companies and governments, identity is about credentials. The best ones, like passports are given more weight than others. However many of these credentials are used to generate others, like credit cards. Interacting online with people from throughout the world is a daily occurrence for millions of internet users, yet most do it with little regard to the personally identifying information they are broadcasting, nor the lack of confirmation of the person or organisation they are engaging with.

In the real world we address this with documents, but how do you verify such documents in the online world? For example, to register with many social sharing sites, all you need is a name (of any description) and a working email account. Other websites, such as wikipedia offer a similar experience for users whether they are registered or not. Online auction sites only require minimal information, most of it unsupported. Yet the vast majority of internet users successfully enjoy all these mediums.

In some e-commerce transactions, accurately verifying a person's identity is critical, however the vast proportion of online activity does not. Even the majority on online trading does not require third party verification, for example, if a buyer does not give their correct address goods will not be rendered to them.

However, the reality is some people provide false or misleading information to these sites. This is incredibly hard to detect and stop. As a result, online identity needs to be looked at differently, not just looking at credentials, but a person's online activity and reputation.

2 What is trust?

Developing trust in another person, an organisation or government may take both an emotional response and a logical act. In the old days (read the late 1990's) trust was mostly to do with e-commerce. To trust a web site enough to enter personal details, such as credit card and address information a set of standards was developed. This included:

- Proving there's a real organisation behind a website (e.g. contact details, about us section);
- Explanation of what that site is going to do with personally identifying information;
- A professional site design; and
- Regular updates the site so it looks alive and fresh.

Unfortunately the rise of phishing and the way it has morphed with both social and technical attacks has been bewildering for many people, subsequently eroding their trust in such technology.

In the online perspective there are generational issues. The I-Pod generation or digital natives are interested in user generated content (which is the foundation of web 2.0). There is an avalanche of new content on the web, the accuracy of which is often largely unknown.

Now the issue of trust has moved away from the people who run the site and is now focused on the people who populate and operate within the site, such as:

- Social sharing platforms (MySpace, You Tube, Second Life);
- Information sites (Wikipedea); and
- Commercial conduits (eBay);

Trust is now being developed by an exchange of goods and ideas. However the values of exchanging trust in the online environment are different because we often do not know what we are receiving, only what we expect. So, trust in the online world means making an exchange with someone (either a person or an organisation) without having full knowledge about them, their intent and the things they are offering to you, whether it is a commercial arrangement or something else.

3 How do we develop trust?

In the real world, the development of trust between culturally disparate organisations and people is a necessary step in the development of a shared basis of action (eg. response to an emergency situation). Behaviour such as sharing world views and life experiences provide an opportunity for people to build a working relationship and a cultural understanding.

The online world is exactly the same. Web 1.0 allowed for web based sharing of information across global and cultural boundaries, including, pictures, stories, maps, etc.

Web 2.0 introduced social networking and discussion technologies, providing a basis for sharing deeper world views and establishing better cultural understanding. This allows for greater ability to realise a persons/organisations values and therefore generate trust quicker and deeper.

To understand an organisation's ideals, you must be able to understand their beliefs and philosophy. Such information needs to be provided with clarity and respect.

Gen Y embrace blogs, etc and are prepared to share themselves thinking that others will share information about themselves.

Organisations can embrace Web 2.0 and those who use it (essentially the next generation of customers, employees and stakeholders) by aligning their values with actions. The question is does an organisations actions align with what they are saying?

People like transacting with organisations who have a good reputation. But how do you create this or in the case of 'bricks n' clicks' organisations transfer this to the online world? eBay use the feedback forum, who don't other e-commerce introduce this functionality? Wikipedia has content provided by volunteers from all over the world and these vast numbers of users edit such content. Like eBay, those who act in ill spirit may be reprimanded. Amazon.com has a reputation system which allows users to judge the value of other people's reviews. This also provides an important tool for users to make value based purchasing judgments. Organisations who 'know' their users can offer a more granular response to them.

If consumers gain confidence about a supplier they will be more inclined to use them, increasing sales and potentially prices. This is how the market works. If a social sharing site contains user postings which are trusted by their community then more people will be driven to use that site.

4 Do we need to be concerned about identity?

The online world of social interaction and commercial transaction is made up of static credentials and reputation. If we know such credentials can be falsified then shouldn't we be more concerned with authenticating a user rather than identifying them?

A significant amount of user data is collected by websites. This includes:

- registration details;
- verification by email address;
- IP addresses (at each login); and
- Purchasing and search behaviour.

This allows for a far greater ability in picking patterns of unusual activity than in the real world. Combine this with clear and regular communications about site's expectations and that of their community and there is a greater chance of creating goodwill.

Authentication can be tailored for each site depending upon the interaction they provide. This can include requiring users to prove one or more of the following:

- What they are (biometric data such as fingerprints);
- What they have (a smartcard or token); and
- What they know (an account name and password).

If internet users consistently authenticate themselves in a range of social and economic transactions, then the trust in their identity will grow and other users and merchants are more likely to want to interact with them. The fact they are authenticating their correct identity is apparent, so they can transfer this trust to real world transactions. This concept also applies to organisations of all sizes.

5 Conclusion

As users move around the chasm of Web 2.0 and transact in social and financial ways their values will be outwardly displayed therefore creating trust in their identity. The sharing of these values is an absolute requirement for the development of trust between individuals and organisations. There are a number of ways websites can seek this aim, including:

- Ensure users continue to trust your site (email, SMS activation upon registration);
- Demonstrate to users they can't operate completely anonymously by telling them you are collecting IP addresses;
- Validate users by considering recommendation from other sites (LinkedIn, eBay);
- Still use original techniques from Web 1.0, but build on them (static pages containing mission and values statements);
- Develop back end modelling and monitoring of e-commerce activity;
- Use tools such as IE7 and other vendor products; and
- Educate your users and customers to protect their identities online and create a mechanism where they can report activity to you which may damage your brand.

References

Bewsell, G.R., Jamieson, R, Gardiner, A., & Bunker, D. (2005) "An Exploratory Investigation of Dispute Resolution Mechanisms: A Domain Study of Online Trust in e-Auctions." *Springer-Verlag Lecture Notes in Computer Science* (Vol 3952/2005).

Bewsell, G. (2005) "Mangoes and Chilli Peppers: A Domain Study of Online Trust in eAuctions." *16th Australasian Conference Information Systems (ACIS),* Nov 30 – Dec 2, Manly, Australia.

22

Schengen Information System II: The balance between civil liberties, security and justice

Katina Michael[1] and MG Michael[2]

[1]Senior Lecturer, School of Information Systems and Technology, University of Wollongong, [2]Honorary Fellow, School of Information Systems and Technology, University of Wollongong

Abstract

This paper investigates the application of the Schengen Information System (SIS) in the European Union and the balance between civil liberties, security and justice. It provides an overview of the SIS, technical issues related to the maintenance of the SIS, and transnational legal issues in the context of national security and public policy. Given that citizens can now move freely between States in Europe, the paper investigates how the SIS is being administered, applied, and enforced and some of the potential problems that arise from cross mutual state recognition of SIS alerts. This paper argues that the SIS has a number of inherent and propagating weaknesses and that the risk exposure presented to citizens is far too great for the benefits that ensue. The paper recommends a movement away from the idea of a fortress Europe toward one of State to State harmonization in transnational criminal issues.

Keywords: Schengen Information System, civil liberties, security, justice

1 What is the Schengen Convention?

The Schengen Agreement was established on the 14th June 1985 when France, Germany, Belgium, Luxembourg and the Netherlands agreed to abolish checks at their common borders, and to create a single external frontier (Council of the European Union, 1999;The European Parliament and the Council of the European Union, 1995).The actual Schengen Convention was ratified in June 1990 and came into effect in March of 1995, by which time several other States had agreed to the EU framework including Italy, Spain, Portugal, and Greece.All signatories agreed to "setting a common visa regime, improving coordination between the police, customs and the judiciary and taking additional steps to combat problems such as terrorism and organized crime" (Justice and Home Affairs,August 2005).

2 What is the Schengen Information System (SIS)?

2.1 The Schengen Information System

The Schengen Information System (SIS) was established in the Schengen Convention (Title IV) (Official Journal of the European Communities, 1999, pp. 439-459).The SIS was operational in 1995, and according to reports collapsed within 90 minutes due to system congestion (Bantekas & Nash, 2003, p. 279).The purpose of the SIS, according to Article 93 of the Convention, is to maintain "public policy and public security, including national security" (Joint Supervisory Authority, n.d.). Given that citizens can now move freely between States in Europe (ie contracting parties only), the information communicated via SIS can help ensure that provisions are met. SIS works on the basis that Member States have a National SIS (N-SIS) which is networked to a Central SIS (C-SIS) (Europa, 2007).Thus the SIS can be considered as a "series of national databases connected to a central system which holds information on suspected criminals, missing persons, unwanted aliens and stolen vehicles and documents" (Bantekas & Nash, 2003, p. 279).

> "In effect it brings together national lists of persons to be excluded from the territory of the Member States into one network, which border guards and visa officials can access online when individuals arrive at the common external border or when they ask for a visa (Guild & Bigo, 2002, p. 129)."

The data on N-SIS and the C-SIS should be identical at any given time. Transborder flows of personal data (TBFPD) are transmitted in accordance with protocols and procedures jointly established by the contracting parties. In its fundamental operation, "[t]he SIS is a database that stores criminal information from participating Member States and is considered to be the most prominent instrument of police co-operation devised under Schengen" (Bantekas & Nash, 2003, pp. 236-237). Compare the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data with the Schengen Convention (Articles 92-101) (Organisation for Economic Co-operation and Development, 1980, p. 9):

> "Data controller means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf; personal data means any information relating to an identified or identifiable individual (data subject); and transborder flows of personal data means movements of personal data across national borders."

2.2 SIS Phase II, SIRENE, Vision, and the SISNET Network

In its original phase I implementation (1995) the Schengen Information System had the capacity to serve no more than 18 participating States (Verwilghen, 2001). Given the expansion of the EU over time, the SIS would need to service more States by 2002 While most official reports identify this as the main reason of the SIS phase II, others believe that it had more to do with the States benefiting "from the latest developments in the field of information technology and to allow for the introduction of new functions" (Iocheva, 2006). It is the latter "new functions" which has concerned privacy advocates in Europe, including organizations like Statewatch (Hayes, 2005). (Hayes, 2004) is clear in his assessment of law enforcement databases, i.e. that they are a product of "original sin". He goes onto add that:

> "*[f]unction creep* is inevitable, regardless of any assurances given by the executive at the time." The notion of privacy is complex. Privacy involves the "social contract between individuals and the society which they live. It invites clashes between individuals and institutions, and between privacy protection and free access to information" (Hoffman, 1979, p. 3).

2.2.1 SIRENE

The Schengen Information System has a supplementary network, known as SIRENE (Supplementary Information Request at the National Entry). SIRENE has been described as a "network trough," and also as the "human interface" of the SIS (European Union, 2002, p. 12). By human interface, it is implied that SIRENE:

> "as a role of first-line contact both for the other SIRENEs and for the national authorities and end users. Depending on the case, SIRENE must be able to deal with it independently or to refer it to the competent authorities or agencies. SIRENE staff should therefore be competent and well-trained and have established good contacts with national and foreign authorities."

SIRENE can exchange additional information to that included in the national portion of the SIS, as well as the C-SIS. In effect SIRENE allows smaller offices within each State to communicate with one another and act as intermediaries between national authorities responsible for the data on SIS such as judges, police and alien offices. It is important to note that the SIS Phase II network is being replaced by the SISNET network (Department of Homeland Security Public Affairs, 26 October 2006). Together these information systems can help national and local police, customs and the judiciary.

3 What information is recorded on the SIS?

3.1 Recorded categories of data

Article 94 of the Convention contains a detailed list of categories of data that can be stored in the system. The categories can be classified into three distinct types: persons, objects, and vehicles. The main objective of SIS is to exchange data on certain categories of people and lost or stolen goods. With respect to persons the following data may be stored: surnames and aliases, physical characteristics not subject to change, date and place of birth, sex, nationality, whether persons concerned are armed or violent, reason for alert, action to be taken. Articles 95-100 stipulate why an alert can be triggered by an official. The reasons include but are not limited to: arrest for the purposes of extradition, to find a missing person whose detention has been ordered, arrest for the purpose of appearing in court, discrete surveillance and specific checks (Article 99), and in the case of aliens who in most cases have not complied with provisions governing entry and residence. With respect to data stored on objects this may include: stolen motor vehicles, firearms which have been misappropriated, blank official documents which have been stolen, issues identity papers which have been stolen and suspect banknotes. While freedom of movement in the EU provides law-abiding citizens with so many benefits, criminals can also take advantage of it for the purposes of terrorism, cybercrime, drug smuggling and firearm trafficking etc. Cross-border crime is also among the most difficult to detect and contain, as several jurisdictions are involved (Justice and Home Affairs, August 2005).

3.2 Who has access to information?

Access to the information on the SIS as stated in Articles 92 and 101 of the Convention can only be by designated authorities for the purpose of border/police/custom checks carried out in the country in accordance with national law. The primary reason for the checks is linked to varying levels of alerts, which may refuse an individual suspected of a crime entry into the designated country. There are regulations governing the type of data to be collected, the content of SIS records including responsibility for their correctness, rules on the duration of alerts, interlinking of alerts and compatibility between alerts, rules on access to SIS data, and rules on the protection of personal data and their control.

It is important to emphasize that "records" today are quite different to the flat-file databases of the past. Duncan (2004, pp. 71, 75) notes:

> "Quite unlike systems of records, today's databases are heterogeneous. They have complex structures determined by the purposes for which they were constructed, and they are plagued by difficulties in

> semantic interoperability because of different vocabularies and different perspectives on the use of the data. Further they are often maintained by multiple sites, are capable of linkage of records across databases, and may not be under the control of a single authority. This makes the application of existing law and administrative procedures problematical. And yet this issue must be addressed because government databases contain highly sensitive and valuable information."

This is particularly true of the SIS, especially given the cross-border nature of it, and the many different languages it traverses including, French, German, Italian, Greek, Finnish, Maltese etc.

4 Technical issues

4.1 The need to standardize practices

The sheer size of the SIS II and the number of Member States now in the European Union requires not only regulation but standardization in practice. "The system can be accessed from 50,000 computers by thousands of police, immigration officers and visa-issuing embassy staff" (Eaglesham, 2000). It is one thing to have a system, with policies, and procedures, and another on how these should be executed in an operational sense (Dalberg, Angelvik, Elvekrok, & Fossberg, 2006). In December 2002, the *Schengen Information System, SIRENE: Recommendations and Best Practices* manual was published so that best practices could be identified serving as "inspiration for the establishment of standards defining the minimum application of the Schengen Acquis" (European Union, 2002, p. 7). It is important to note, that after the introduction of SIS II in 2001, SIS I and SIS II were considered one and the same. Of utmost important in SIS was ensuring the balance between the number of alerts entered into the system, and that the alerts inserted were of good quality.

> "Every national alert that is "Schengen relevant" should in principle be introduced in the SIS. However, in order to be able to execute the alert, it is necessary that the alert is correct, as complete as possible and traceable. Finally, it should be borne in mind that when a Schengen State executes an alert, it has the right to expect that the issuing Schengen State will follow up the hit. Not doing so without a valid (legal) reason will negatively impact on the willingness of (local) authorities to use the SIS and maximize its potential" (European Union, 2002, p. 11).

4.2 System maintenance, real-time updates and offline copies

A great number of technical issues abound in such a monolithic system such as the SIS that covers a great deal of Europe 'physically' and has so many people 'accessing' it and 'updating' and 'maintaining' it. Beyond the day-to-day issues of hardware and software required to operate the system 24/7, there is the need to maintain that the data shown to the end-user is in fact a true copy of the current state of affairs. For instance, it is quite possible that an alert has been changed from "high" to "low" or from "low" to "no longer valid" and this kind of change needs to be reflected in all N-SIS/C-SIS in real-time. To this end, regular automated database comparisons are required. Where on-line access to the data is not possible, regular off-line copies need to be sent and additional phone checks made. This does pose a security risk in itself- especially when it has been noted that whole databases on CD-ROM are sent regularly to Consulates (W. van de Rijt). In November of 1997, SIS data was found at a Belgian railway station accidentally left behind by an official (Eaglesham, 2000, p. 24).

4.3 Dealing with coordination issues between agencies

Coordination is a problem often cited but has been to some extent overcome by the function of SIRENE to act as a single point of contact for each Schengen State. For this matter the management structure needs to be standardized as well. Where several authorities are involved in a particular case where alerts may be conflicting, eg the Schengen State authorities and Interpol, the Schengen alerts always take precedence. In this instance, Interpol would be required to provide the Schengen State with a Schengen ID alert. Again the importance of well-trained administrative and operational staff is that they add to the robustness of the system and ensuring efficient workflow (European Union, 2002, pp. 14-15). It is also important that SIRENE offices are armed with competent legal expertise and are conversant in the appropriate languages (especially of their bordering States and of course, English).

4.4 User interface issues and data quality

From a user interface perspective, the query functionality provided by the software needs to go beyond "exact match searching" to include "phonetic queries, wildcard queries, fuzzy logic, soundex" (European Union, 2002, p. 18). Data quality of pre-existing national data on an individual should be checked for Schengen relevance and correctness before being loaded into the central SIS or into newer systems. Alerts and actions should be clearly communicated to end-users. For instance, in the case of misused identity, the procedure to deal with a given *hit* and the subsequent investigations required should make it known whether the individual in question is the victim of identity fraud, or the perpetrator of the misuse. Consider the case where an Ethiopian citizen living in Budapest who was refused admission to France because his name was entered on the SIS in Germany after he reported a missing passport. It took eight months to get the information corrected (Eaglesham, 2000).

4.5 Data handling issues and alerts

Beyond data quality is the issue of data handling. In the event an alert is recorded, it should satisfy the criteria of the Schengen Convention in accordance to Article 95, to ensure a *hit* will be followed up. If an alert is identified as invalid, SIRENE operators should have the capability to delete it. In the same token, when an alert is extended, its on-going validity should be re-examined, and a reply to that given case should be provided in the shortest possible time. For instance, when one Schengen State alerts another Schengen State of a positive response on a given alert, it is a *hit*, and these should also be recorded. Each alert should have a separate Schengen ID number allotted to it to ensure that audits of events are possible and also to minimize confusion between the States. Operators should not fill in mandatory fields with words like "unknown" as this renders untraceable information, in the same token it is important that operators act ethically to ensure that they are not documenting things that are not reflective of evidence.

4.6 The growing need for security policies

All these technical issues do lend themselves to a security policy which is standardized across all of the Schengen information technology (IT) systems. Who has access to these systems, at what appropriate level and for how long, is something that is not easy to solve. Indeed this is one of the major problems identified by experts regarding monolithic systems such as the SIS. There are no easy answers to this issue, only to ensure that SIRENE recruit responsible personnel with the appropriate clearance and certification. In terms of physical security, the SIS has computers located underground, differing security zones, staff use access cards for entry, there are armed-guards and closed circuit television monitoring (CCTV) at entries and exits (European Union, 2002, p. 30). Staff also have unique IDs and passwords to log onto the systems securely.

5 Legal issues

5.1 Cross mutual recognition versus harmonization

The SIS is fraught with well-known legal issues. According to Minas Samatas (2003, p. 141):

> "[t]he more serious implementation problems of the SIS are the legal
> ones – regarding the protection of citizens' privacy and civil liberties,
> as well as the human rights of foreigners."

At the first instance, the SIS is populated by individual Schengen States according to a national understanding of the criteria for inclusion and a national interpretation of public order and security. "The underlying principle of the system is based on the notion of cross mutual recognition of national decisions rather than harmonization" (Guild & Bigo, 2002, p. 126). For instance, if a person is deemed to have acted inappropriately in one Member State and their personal data is subsequently recorded in the SIS (while the individual is still in that territory), then other Member States need to act upon that 'alert'. However, what one Member State deems a "risk", another Member State may not, yet they are still bound to the Schengen Convention.

What is perceived as a security risk in one state is not necessarily the same in another. This difference of perception of the notion within the Union will be the territory where national courts begin to question the legitimacy of the system

(Guild & Bigo, 2002, p. 129).

5.2 The Visa List and profiling for potential criminals

Many legal representatives across the globe see another fundamental error with the SIS- it not only is used for outright 'exclusion' of an individual from the EU based on one Member State's understanding of the criteria, but it also can identify 'groups' of persons who supposedly pose a greater risk to the EU based on their nationality as depicted on the 'visa list' (Harper, 2006). It should be highlighted that these are individuals who have done nothing wrong, have been in an EU Member territory for some time, and who would have otherwise been entitled to freedom of movement within the EU exterior border, but who for the fact that they have been born in a particular country, are categorized as being 'more' or 'less' likely to be a risk (Guild & Bigo, 2002, p. 127). By controlling the individual through a visa requirement, jurisdictional issues are placed back in the hands of the individual's own State (Department of Homeland Security Public Affairs, 2006). Profiling techniques are used on these groups, and individuals anticipated to be 'a criminal' (or who may become a criminal over time) are excluded (Strandburg & Raicu, 2006). There are fundamental problems with this- who actually defines what constitutes a risk to security? It should also be noted that until the mid-1980s visas were regarded as "expressions of mistrust", especially of non-EU migrants (Anderson & Apap, 2002, p. 247).

5.3 Human rights versus a 'Fortress Europe'

If the basis for what information can be entered into the SIS is national law, then a National-SIS (N-SIS) may make complete sense, but a patchwork of national lists brought together in a Central-SIS (C-SIS) may not.

> "This means by which the authorities of a Member State come to the decision to enter the data are under the exclusive control of the Member State authorities. Thus a Member State could have other reasons than security to include a person on the list and this would not breach Article 96… There is no attempt to restrict or harmonize what is permissible at the national level. But whatever happens at that level is then to be recognized as value by the other States" (Guild & Bigo, 2002, p. 131).

To illustrate this point, consider the number of records in the central SIS as of May 23, 2000 was 9.7 million. The country with the most entries about persons was Germany. During this period, there was a perceived threat to Germany by 'foreigners' which constituted both asylum seekers, and ethnic Germans from Central and Eastern Europe (known as *Aussielder*). This caused quite a bit of public disquiet to the measure that asylum seekers, now considered outright foreigners, were entered into the SIS because they were seen as a "risk category". France on the other hand, at the time, had a different view on asylum but still had to reject the persons who had been inserted into the SIS. This kind of perceived misuse of the SIS is in direct conflict with the obligation of Member States to "provide protection to persons fearing persecution and torture" (Guild & Bigo, 2002, p. 134).

6 Transnational issues

When considering a system like the Central Schengen Information System, by its very nature, it poses transnational challenges (House of Lords, 2007). It is an information system that traverses a great number of national borders and therefore jurisdictions, and as a result is subject to harmonization problems. At the heart of the problem is the principle of equality of treatment, human rights, and the function of the State within the context of the EU ((Electronic Privacy Information Centre & Privacy International, 2003, p. 59). According to (Samatas, 2003, p. 141): "[i]t is clearly an 'immigration anathema' to build a 'Fortress Europe', especially as regards Third World immigrants' and refugees' rights and life chances in the EU."

'Security' and 'risk' will always mean different things to each Member State, and no amount of 'best practice' literature will ever eradicate this issue. While in theory the C-SIS can help to facilitate and minimize crime in the EU, by increasing cooperation and knowledge sharing between Member States and respective authorities down to the local level, it sends conflicting messages regarding principles and standards documented in the European Convention on Human Rights and within an international law context. This type of *Europeanization* may also end up contributing to the erosion of national sovereignty (Boer, 2002, p. 152).

7 Freedom, security and justice in the EU

There is no doubt that the European Union has tried to provide internal security for its law-abiding citizens, to move freely between Member States, and to enjoy the stability, wealth and internal liberal environment. Ironically, however this requirement to ensure 'security' has come at the expense of 'freedom'; with the erosion of freedom has also come the problem of 'justice'. This means that a greater balance must be struck between opposing forces which are at play. Monar (2002, p. 167) cite one example of this balance needing to be struck with the

> "EU measures in the fight against cross-border crime and illegal immigration, which now involves a range of major EU-wide data-bases, [and which] must respect high standards in terms of the protection of personal data and comply with strict rules on the interception of telecommunications and other investigative techniques…"

If the protection of personal data is not maintained appropriately, for instance in the quite plausible scenario that persons may accidentally or deliberately (Fijnaut, 2002, p. 219) be named on the C-SIS by a Member State when they are in actual fact innocent of any crime, then there is clearly a fundamental erosion of human rights at play.

> "For Euro-skeptics and human rights activists, on the other hand, a serious concern over the SIS is whether its function will diminish the

> protection of civil liberties and human rights in countries like Greece, which have an authoritarian state culture and a rather negative historical record on human rights" (Samatas, 2003, p. 147).

The reality is that there can never be a balance between freedom, security and justice where these types of monolithic information systems exist. While freedom has to do with an individual's 'privacy' (ie autonomy, self-possession, integrity) (Garfinkel, 2000, p. 5), 'security' has to do primarily with the State, and justice is supposed to ensure some kind of balance. The bigger these systems get, the more potential there is for error, especially given the nature of transborder personal data flows. This does not negate of course, the obvious benefits that these systems have contributed, especially for law enforcement agencies in the tracking of stolen vehicles and other like objects but these benefits do not in themselves remove the deep-rooted problems pertaining to data quality, data correctness, breaches in personal privacy, access to information in the SIS II and beyond.[1] While it is the role of the Joint Supervisory Authority (JSA) on Schengen to maintain data protection of the SIS and new emerging networks, they are there only within a supervisory capacity with little 'authority' to enact change (Joint Supervisory Authority, 2004, June 2005; Secretariat, 2007). There is here a concluding call for more protective mechanisms and access controls[2] to be put in place, including technical regulations which are binding to Member States, beyond guidelines.[3]

[1] The debate between an individual's privacy and the security of the state continues. According to (Crosbie, 2006): 'We never get any evaluations on the effectiveness or a data-privacy cost-benefit analysis. But if you oppose this you are said to be soft on terrorism and you are endangering the fight on terrorism.' The effectiveness of the system in terms of 'hit' rate (ie alert, action, response) is also under question. See also (Bantekas & Nash, 2003) p. 280: 'The successful 'hit rate' of the system is generally low and it is questionable whether the information held on the SIS is accurate. The data protection provisions of this system, which holds approximately 9.7 million files, have been subjected to severe criticism.'

[2] 'In addition to avoiding formal procedures, prosecuting authorities engage in informal mutual co-operation practices by simply allowing police officers in another jurisdiction access to evidence' (Bantekas & Nash, 2003) p. 259. At present it is this informal cooperation which needs to be formalized.

[3] 'In the last few decades, law enforcement and intelligence cooperation has significantly increased. They are an important form of international cooperation… [but] there are no treaties applicable to law enforcement and intelligence cooperation… nor are there such forms of information-gathering and information-sharing by and between different agencies within separate countries. Regrettably, this important form of international cooperation has not yet been included in mutual legal assistance treaties. Consequently, there are no legal or judicial safeguards to insure effective and regulated modalities of information-gathering and information-sharing between intelligence, law enforcement, and prosecutorial agencies. Thus effectiveness is reduced and potential abuses are increased. This affects the accuracy of the information, and can lead to undue invasion of privacy. Because these practices are internationally unregulated, and nationally unmonitored by the judiciary when committed other than on the national territory, they pose a challenge to due process of law and to the right of privacy' (Bassiouni, 2003), pp. 368-369.

References

Anderson, M., & Apap, J. (2002). *Police and Justice Co-operation and the New European Borders*. London: Kluwer Law International.

Bantekas, I., & Nash, S. (2003). *International Criminal Law*. London: Cavendish.

Bassiouni, M. C. (2003). *Introduction to International Criminal Law*. New York: Transnational Publishers.

Boer, M. D. (2002). Intelligence Exchange and the Control of Organised Crime. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and The New European Borders* (pp. 151-161). The Hague: Kluwer Law International.

Council of the European Union. (1999). *8415/99 Limite Schengen 52*.

Crosbie, J. (2006). EU regulations: MEPs seek to restrict police access to visa data. *The Economist Intelligence Unit Ltd*.

Dalberg, V., Angelvik, E., Elvekrok, D. R., & Fossberg, A. K. (2006). *Cross-cultural Collaboration in ICT Procurement* Paper presented at the Proceedings of the 2006 International Workshop on Global Software Development for the Practitioner Shanghai, China.

Department of Homeland Security Public Affairs. (26 October 2006). The United States Mission to the European Union. Retrieved 9 October 2007, from http://www.useu.usmission.gov/Dossiers/Travel_Documents/Oct2606_ePassport_VWP.asp

Department of Homeland Security Public Affairs. (2006). The United States Mission to the European Union. 26 October. Retrieved 9 October 2007, from http://www.useu.usmission.gov/Dossiers/Travel_Documents/Oct2606_ePassport_VWP.asp

Duncan, G. T. (2004). Exploring the Tension Between Privacy and the Social Benefits of Government Databases. In P. M. Shane, J. Podesta & R. C. Leone (Eds.), *A Little Knowledge: Privacy, Security, and Public Information after September 11* (pp. 71-88). New York: The Century Foundation Press.

Eaglesham, J. (2000). EU's Largest Database 'Contains Serious Flaws' Human Rights Pressure Groups Call for Inquiry. *Financial Times*.

Electronic Privacy Information Centre, & Privacy International. (2003). *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*. New York: EPIC, PI.

Europa. (2007). Member States of the EU. Retrieved 12 October 2007, from http://europa.eu/abc/european_countries/index_en.htm

European Union. (2002). *Volume 2: Schengen Information System: SIRENE: Recommendation and Best Practices*.

Fijnaut, C. (2002). The Problem of Corruption of Police Officials. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 219-226). The Hague: Kluwer Law International.

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. Beijing: O'Reilly.

Guild, E., & Bigo, D. (2002). The Schengen Border System and Enlargement. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 121-138). The Hague: Kluwer Law International.

Harper, J. (2006). *Identity Crisis: How Identification is Overused and Misunderstood*. Washington: CATO Institute.

Hayes, B. (2004). From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained. Retrieved 29 May 2007, 2007

Hayes, B. (2005). SIS II: Fait Accompli? Construction of EU's Big Brother Database Underway. Retrieved 28 May 2007, 2007, from http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf

Hoffman, L. J. (1979). A Research Agenda for Privacy in the Next Decade. In L. J. Hoffman (Ed.), *Computers and Privacy in the Next Decade* (pp. 3-6). Sydney: Academic Press.

House of Lords. (2007). *Schengen Information System II (SIS II): Report with Evidence (9th Report of Session 2006-07).* London: The Stationary Office Limited.

Iocheva, M. (2006). European Parliament Backs Compromise to Extend Schengen Information System to New Member States. *US Fed News Services.*

Joint Supervisory Authority. (2004). Opinion on the Development of the SIS II. Retrieved 11 October 2007, from http://www.cnpd.pt/bin/actividade/SISII_opinion.pdf

Joint Supervisory Authority. (June 2005). ARTICLE 96 INSPECTION: Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System. Retrieved 11 October 2007, from http://www.statewatch.org/news/2005/sep/jsa-sis-art96-rep.pdf

Joint Supervisory Authority. (n.d.). The Schengen Information System. Retrieved 17 September 2007, from http://www.garanteprivacy.it/garante/navig/schengen/jsp/main.jsp?

Justice and Home Affairs. (August 2005). Schengen Convention: Abolition of Internal Borders and Creation of a Single EU External Frontier. Retrieved 11 October 2007, from http://ec.europa.eu/justice_home/fsj/freetravel/frontiers/wai/fsj_freetravel_schengen_en.htm

Monar, J. (2002). The Problems of Balance in EU Justice and Home Affairs and the Impact of 11 September. In M. Anderson & J. Apap (Eds.), *Police and Justice Co-operation and the New European Borders* (pp. 165-182). The Hague: Kluwer Law International.

Official Journal of the European Communities. (1999). *The Schengen Acquis.*

Organisation for Economic Co-operation and Development. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD.

Samatas, M. (2003). Greece in 'Schengenland': blessing or anathema for citizens' and foreigners' rights? . *Journal of Ethnic and Migration Studies, 29*(1), 141-156.

Secretariat, D. P. (2007). The Joint Supervisory Authority of Schengen Retrieved 10 October 2007, from http://www.schengen-jsa.dataprotection.org/

Strandburg, K., & Raicu, D. S. (2006). *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation.* New York: Springer.

The European Parliament and the Council of the European Union. (1995). *Protocol Integrating the Schengen Acquis in the Framework of the European Union.*

Verwilghen, M. (2001). *Council Regulation (EC) No 2424/2001 of 6 December 2001 on the Development of the Second Generation Schengen Information System (SIS II)*: Official Journal of the European Communities.

W. van de Rijt. (7-8 December 2000). *Council of the European Union.* Paper presented at the ERA Seminar: Schengen in the Nordic States, Helsinki.

Author Biographies

Ms Roba Abbas graduated with first class honours in Information and Communication Technology (majoring in Business Information Systems) from the University of Wollongong, in 2006. She is currently the Product Manager at Wollongong-based web software development company Internetrix, and is involved in the areas of consulting, and product sales, research, development and improvement. Roba's primary research interest lies in the critical infrastructure protection area, with a particular focus on the impact of public data availability on critical infrastructure protection efforts in Australia. Ms Abbas has attended two RNSA Workshops to present her research in this field. Her honours thesis is available at http://ro.uow.edu.au/thesesinfo/2/ · roba06@gmail.com

Mr Anas Aloudat is a PhD candidate in the School of Information Systems and Technology at the Faculty of Informatics at the University of Wollongong. His thesis is investigating user acceptance of location based services in emergency management within Australia. Mr Aloudat holds a Master of Science in Computing from the University of Technology, Sydney and a Bachelor of Science in Computer Science from Mu'tah University in Karak, Jordan. He is presently a sessional tutor at the University of Wollongong where he has taught topics in eBusiness and location based services. Between 2000 and 2002 Mr Aloudat was also a computer lab assistant in the Faculty of Science at Mu'tah University. He was recently made a member of the Cellular Emergency Advisory Service Association (CEASA), and has been a member of the Research Network for a Secure Australia since 2006. He is also a reviewer of the *Journal of Theoretical and Applied Electronic Commerce Research* (JTAER). aloudat@gmail.com

Mr Mark Burdon is a PhD candidate in the Faculty of Law at QUT. His thesis is investigating whether the commercial re-use of public sector information in Australia affects the information privacy of Australian citizens. Mark has a law degree from London South Bank University and a Masters degree in Public Policy from the University of London's Queen Mary and Westfield College. Since 2005, Mark has worked on a diverse range of legal/socio/technology related projects with QUT's Information Security Institute (ISI) involving the reporting of data breaches, e-government information frameworks, consumer protection in e-commerce and information protection standards for e-courts. m.burdon@qut.edu.au

Mr Steven R. Clark is a PhD Candidate at the University of South Australia. His doctoral research lies at the intersection of law and technology, examining privacy and data integrity issues in government identity management systems. Previous research includes media propaganda as a crime against humanity, hypermedia database design issues, and DNA repair mechanisms. Steven has broad experience across ICT; including software and hardware support and development, education, and management. In legal practice he has worked in criminal defence and civil litigation, in private practice and the South Australian Crown Solicitor's Office. He holds a BSc(Hons) in Molecular Biology and a LLB/LP(Hons) from Flinders University, with postgraduate studies in Computer Science, International Criminal Law, and in Education. He is a Member of the Australian Computer Society, the Law Society of South Australia, and other professional and community organisations. Steven.Clark@unisa.edu.au

Professor Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and a Visiting Professor in the Department of Computer Science at the Australian National University. He was for a decade the Chair of the *Economic Legal and Social Implications Committee of the Australian Computer Society,* and spent some time as the ACS Director of Community Affairs. He holds degrees from UNSW and ANU, and has been a Fellow of the ACS since 1986. He has been a Board-member of the *Australian Privacy Foundation* since its foundation in 1987, and its Chair since 2006. He has undertaken research, consultancy and public interest advocacy, and published extensively in Australia and overseas for over 30 years, in the areas of identification, security, dataveillance and social impacts and implications of information technology. His website is one of the most extensive and most used resources in these areas. Roger.Clarke@xamax.com.au

Ms Suzanne Lockhart is a criminologist with extensive practical and theoretical experience of the Australian criminal justice system spanning twenty years, specializing in identity crime, criminal intelligence, biometric technology and national security in mission critical public and private sector organizations. She has been a sworn member of the Victoria Police and the Australian Federal Police. She has a Criminal Justice Administration degree and a M.A. Criminology degree from the University of Melbourne, which researched the alignment between organizational requirements and end user perspectives of biometric technology. She has specialized training in criminal profiling, identity crime and biometric technology and is undertaking an Australian Research Council and Australian Transactions Reports and Analysis Centre (AUSTRAC) sponsored PhD researching identity crime solutions, biometrics; displacement effects and diffusion of benefits. Suzanne has extensive project management expertise within the intelligence, fraud and national security environment in Australia and overseas and has strong affiliations with international research institutions and close contact with many public and private sector organizations. Suzanne is the Australian representative on the International Organisation for Standards (ISO) SC37 Biometric Working Group

6, Cross Jurisdictional and Societal Issues committee and is a technical consultant for the Australian Biometrics Institute Technical Committee. Suzanne also consults and provides industry training in the area of biometrics, identity crime, intelligence analysis, identity management and homeland security for academic institutions and public and private sector organizations. She has also been the Senior Intelligence Analyst and the National Manager of the Australian Identity Protection Register, Australian Crime Commission and is currently the Assistant Director, Information Coordination Branch, Protective Security Coordination Centre, Attorney-General's Department. suzanne@biometricconsulting.com.au

Mr Mark Loves is a former Detective Sergeant (NSW Police) with extensive experience in criminal investigation and intelligence. During his police service he worked on numerous high profile investigations, including the Milperra Bikie massacre, and was twice awarded by the International Association of Law Enforcement Intelligence Analysts for excellence in the criminal intelligence field. Following the police, he spent eleven years as National Corporate Security Manager for Optus/SingTel, during which time he was appointed by Attorney General (Hon.) Phillip Ruddock to the Prime Minister's Critical Infrastructure Advisory Council (CIAC). It was also during this period that he instigated an investigation which led to the first ever conviction for computer hacking in Australian history (Dendtler's case). He is currently a Senior Lecturer with the University of Wollongong's Centre for Transnational Crime Prevention where he lectures on security, intelligence and policy, as well as representing the Centre in international forums. mloves@uow.edu.au

Professor Chris B. Del Mar BSc MA MB BChir MD FRACGP FAFPHM is Dean of Health Sciences and Medicine, and PVC (Research), at Bond University, Gold Coast, Queensland. Following his education in science, and then medicine (at Cambridge, UK), and working in London he moved to Mackay, North Queensland in 1977. He became a full time general practitioner there, working in his own practice until 1988, when he took up an academic position at the University of Queensland in Brisbane. He was professor of general practice at the University of Queensland 1995-2004. He has undertaken research into health services and also clinical areas. He has published over 200 research papers, reviews, book chapter and books. He is a Coordinating Editor of the international *Cochrane Collaboration,* and was Editor of the research section of the *Australian Family Physician,* Chair of the Royal Australian College of General Practitioners (RACGP) National Research Committee, and President of the Australian Association for Academic General Practice. He chairs the editorial committee of the Australian Government's health web portal, *HealthInsite*. He was appointed visiting professor of general practice at Oxford University in 2007. cdelmar@bond.edu.au

Dr Greg Marston is Senior Lecturer, School of Social Work and Human Services, The University of Queensland. Greg's research interests cover social security policies, contemporary social theory and the politics of policy making. He has written numerous articles on social policy and social change and has published two books on social policy and social theory. g.marston@social.uq.edu.au

Dr Katina Michael PhD (UOW) 2003, BIT (UTS) 1996, Senior Member IEEE '04. Katina is on the *IEEE Technology and Society Magazine* editorial board, and is the technical editor of the *Journal of Theoretical and Applied Electronic Commerce Research.* Her research interests are in the area of location-based services, emerging mobile technologies, national security, and their respective socio-ethical implications. Katina is currently a senior lecturer in the School of Information Systems and Technology, Faculty of Informatics, University of Wollongong, Australia. She teaches eBusiness, strategy, innovation and communication security issues, and is the research administrator of the IP Location Based Services Program. Katina has authored over 50 refereed papers and is currently working towards the completion of her fourth book. In 2007 Katina was awarded an Australian Research Council Discovery grant for the project: 'Toward the Regulation of the Location-Based Services Industry: Influencing Australian Government Telecommunications Policy' valued at $192K. She has held several industry positions including as a senior network and business planner for Nortel Networks (1996-2001). In her role with Nortel she had the opportunity to consult to telecommunication carriers throughout Asia. katina@uow.edu.au · http://ro.uow.edu.au/kmichael

Dr M.G. Michael Ph.D, MA(Hons), MTh, BTh, BA is a theologian and historian who brings a unique perspective on Information Technology and Computer Science. Presently he is an honorary fellow in the School of Information Systems and Technology, at the University of Wollongong, Australia. He is the former coordinator of Information & Communication Security Issues and since 2005 has guest-lectured and tutored in Location-Based Services, IT & Citizen Rights, Principles of eBusiness, and IT & Innovation. He has presented papers at numerous IEEE conferences including the *International Conference on Mobile Business,* the *International Conference on Mobile Computing and Ubiquitous Networking,* and *RFID Eurasia*. In 2000 he was invited to present a paper "Revelation 20:4-5 Chiliasm in the Early Ecclesiastical Writers', at the *Millennium Conference on the Sea of Galilee and the City of Jerusalem (Israel).* More recently he delivered a paper at the *29th International Conference of Data Protection and Privacy Commissioners* (ubiquitous computing track) in Canada. He is currently co-authoring a book titled, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants.* Alongside Katina Michael he has introduced the concepts of 'überveillance' and 'electrophorus' into the privacy and bioethics literature. Michael has been the recipient of a number of scholarships and awards. He is a member of the American Academy of Religion. mgm@uow.edu.au · http://ro.uow.edu.au/mgmichael

Mr George Mickhail, Senior Lecturer, School of Accounting and Finance, Faculty of Commerce, University of Wollongong. He was trained in Commerce and Computer Science at Ain Shams University (Egypt), Operations Research at the Sadat Academy for Management Sciences (Egypt), and in Information Systems at the London School of Economics and Political Science (UK). He holds a 'Professeur des Universites Etranger' appointment at the Universite' D'Orleans (France) concurrently with his permanent appointment at the University of Wollongong, which he joined in 1994, after being at The University of Sydney for four years. Prior to academe, George held accounting and consulting appointments with a number of global firms and continues to collaborate with industry and the profession. His primary research exploits semiotics and autonomic computing for autonomic accounting applications (AAA), as a practical proposition for implementing efficiency within organisations. His secondary research critically examines how those new business and technological models utilise IT developments to create –or deplete- value in organisations. The research particularly evaluates the efficiency imperative in the e-transformation of the role of government, business and markets and their global effect on the individual and society. george@uow.edu.au

Mr Rob Nicholls is an independent consultant who works with Gilbert + Tobin. He is a communications specialist with a 25 year career focusing on technology, regulatory and business strategy in broadcasting and telecommunications. He has an extensive technical and regulatory background which he combines with commercial, finance and analytical experience. Rob currently works in Asia, the Middle East and Europe as well as in Australia. He is widely published and regularly presents at local and international conferences in the fields of regulation, telecommunications and broadcasting. Rob has an honours degree in Electronics and Communications Engineering from Birmingham University and a Master of Arts in International Relations at UNSW. He is currently a PhD candidate at UNSW in the field of the global politics of the regulation of broadcasting. rnicholls@gtlaw.com.au

Associate Professor Nick O'Brien specialises in Counter Terrorism. He is a member of Australian Graduate School of Policing, Faculty of Arts at Charles Sturt University (CSU). Before joining Charles Sturt University (CSU), Nick represented the UK Association of Chief Police Officers - Terrorism and Allied Matters Committee (ACPO-TAM) as the Counter Terrorism and Extremism Liaison Officer (CTELO) at the British High Commission in Canberra. Nick covered Australasia and had a 'watching brief' on the Asia and the Pacific region. Prior to this posting Nick was in charge of International Counter Terrorism in Special Branch at New Scotland Yard, London. Nick has also represented the UK at Europol, the G8 Counter Terrorism Practitioners meetings and the European Police Working Group on Terrorism. Nick is a visiting Fellow at the Jakarta Centre for Law Enforcement Co-operation in Indonesia. Nick first started working in the counter terrorism related area in 1981 and has worked on Irish as well as international terrorism. nobrien@csu.edu.au

Mr Nigel Phair is the Principal of eSecurity Consulting (www.esecurity.net.au), an Australian based organisation which specialises in providing information security advice, intelligence and training. He has extensive experience working with a variety of industry groups, including banking & finance and the telecommunications sector. He is a Lecturer within the Centre for Transnational Crime Prevention, University of Wollongong and a Lecturer at Charles Sturt University. Nigel holds a Bachelor of Administrative Leadership degree and a Masters of Public Policy degree from the University of New England, and a Master of Laws from the Australian National University. He is a Graduate of the Australian Institute of Company Directors and has published an acclaimed book on the international impact of cyber crime. Nigel.Phair@gmail.com

Dr Lucy Resnyansky - Research Scientist, Command, Control, Communications & Intelligence Division (C3ID), Defence Science and Technology Organisation (DSTO), Australia. She has a PhD in Social Philosophy (1994) from Novosibirsk State University (Russia) and a PhD in Education (2005) from the University of South Australia. Her research experience covers studies of language as an instrument of power and influencing public opinion; computer-mediated communication; and discourse analysis of multimodal texts. Current research interests are in the areas of social modelling, epistemological aspects of multidisciplinary research, cross-cultural communication, sociocultural implications of technology, and use of ICT-mediated information sources. These issues are approached from the perspective of sociology of science, philosophy of technology, activity theory, semiotics and discourse theory. Lucy.Resnyansky@dsto.defence.gov.au

Dr Mark Rix is a Senior Lecturer in the Graduate School of Business at the University of Wollongong where he teaches subjects in the areas of organisational behaviour and international human resource management. Mark's research interests are mainly in the field of public policy and public administration, with a focus on issues relating to social exclusion, access to justice and citizenship. He also conducts research on the implications of anti-terrorism legislation in Australia, Great Britain, the United States, Canada and New Zealand for human rights and the rule of law in these countries. Mark has recently had articles on his research published in *Prometheus, Australian Journal of Public Administration, Alternative Law Journal, Third Sector Review, Australia and New Zealand Health Policy, and the Journal of Higher Education Policy and Management.* mrix@uow.edu.au

Ms Michelle Rowland is a lawyer at Gilbert + Tobin. She specialises in a broad range regulatory and commercial telecommunications law including interconnection, privacy, law enforcement, disputes and submissions to government and regulator inquiries. Michelle has a working knowledge of Australia's telecommunications regulatory environment, having completed extended secondments in-house to some of Australia's leading telco providers. Michelle also has a broad range of international communications expertise. This includes best practice regulatory design and legislative drafting, particularly in emerging economies, representing operators, investors, governments and regulators. Michelle has a Bachelor of Arts (Hons), a Bachelor of Laws and a Master of Laws, each from the University of Sydney. Michelle was awarded the 2004 Gilbert + Tobin Scholarship for a course in utility regulation at the Public Utility Research Centre, University of Florida. Michelle serves as Councillor and Deputy Mayor of Blacktown City Council, the largest local government area in New South Wales. mrowland@gtlaw.com.au

Dr Holly Tootell is a Lecturer in the School of Information Systems and Technology, Faculty of Informatics at the University of Wollongong where she teaches in the areas of social implications of information technology and innovation. Holly's research interests are the intersection of privacy, security and liberty in relation to information technology. Her PhD explored these issues with a focus on national security. Holly is a Board Member of the *Australian Privacy Foundation* and is the Secretary of the Australian Chapter of the *IEEE Society on Social Implications of Technology (SSIT).* holly@uow.edu.au

Mr David Vaile became the Cyberspace Law and Policy Centre's first executive director in 2002. He coordinates the Centre's support for ARC research projects such as Unlocking IP, Interpreting Privacy Principles and Regulating Online Investing, and teaches Cyberspace Law and Law in the Information Age. His background in law, IT and communications includes legal research (Legal Aid NSW), data protection (Privacy Commissioner's Office), pro bono, public interest and test case litigation (Public Interest Advocacy Centre), a virtual community for advocates (with the Law Foundation of NSW), organisational governance, database development, and online professional education. His research interests in cyberspace law and policy include privacy and data protection, IT security, jurisdiction online, copyright and digital intellectual property, e-health, risk management and user-centred design. He is also a member of the Information Security World Advisory Board, and the board of the *Australian Privacy Foundation.* d.vaile@unsw.edu.au

Mr Samuel Fosso Wamba is a lecturer in the School of Information Systems & Technology at the University of Wollongong. Prior to this, he was a part-time professor at the School of Business of Ottawa University and a lecturer in the School of Information Technology of Sherbrooke University in Canada. Fosso Wamba has a Masters Degree in Mathematics from Sherbrooke University and a Masters Degree in e-commerce and computer science from HEC of Montreal. Mr. Wamba is nearing completion of a PhD in industrial engineering at the Polytechnic School of Montreal, Canada. His current research interests are in the area of RFID technology and the EPC Network. He has been published in top academic journals and conferences such as *International Journal of Production Economics, Journal of Theoretical and Applied Electronic Commerce Research, Hawaii International Conference on System Sciences and Americas Conference on Information Systems.* He is also the co-author of a chapter in the forthcoming book *"RFID Handbook: Applications, Technology, Security and Privacy".* Samuel Fosso Wamba is a CompTIA RFID+ Certified Professional and Academic Founder of *Academia RFID,* a world leading company on RFID technology. samuel@uow.edu.au

Professor Robert Watts is Discipline Leader Social Sciences, School of Global Studies, Social Science and Planning. Professor of Social Policy in the School of Global Studies Social Sciences and Planning. After teaching at Latrobe University and the University of Melbourne in the 1970s he taught in CAES in Melbourne and in Canada and also helped establish what became Victoria University in 1987. He has been with RMIT since 1993-4. Rob is passionate about the role and responsibilities of the modern university. He is also passionate about the need to do research that makes a difference. Rob has written many books and articles on a range of topics drawing on a wide range of social theories. rob.watts@rmit.edu.au

Professor Marcus Wigan (http://go.to/.mwigan) is Principal of Oxford Systematics, Professorial Fellow at the University of Melbourne, Professor of both Transport and of Information Systems at Napier University Edinburgh and Visiting Professor at Imperial College London and serves on the *Ethics Task Force and the Economic Legal and Social Implications Committee of the Australian Computer Society,* of which he is a Fellow. He has worked on the societal aspects of transport, surveillance and privacy both as an engineer and policy analyst and as an organisational psychologist. He has published for over 30 years on the interactions between intellectual property, identity and data integration in electronic road pricing and intelligent transport systems for both freight and passenger movements. He is spokesman for the *Australian Privacy Foundation* on transport issues, and works with the University of Melbourne on transport engineering and information issues in both logistics and social and environmental factors. His recent work in Scotland has been focussed on data observatories, knowledge management and transport informatics, currently as part of a European Union railway project in London on the issues of a national transport data infrastructure; in Australia he has also worked on vehicle identification and related issues. oxsys@optusnet.com.au

Workshop Participants 2006-2008

Authors

Ms Roba Abbas I, II, III
Mr Anas Aloudat III
Professor Mary Barrett I
Ms Emilia Pérez Belleboni I
Mr Jesús Moreno Blázquez I
Professor Simon Bronitt I
Mr Mark Burdon I, II, III
Mr Steven R. Clark III
Professor Roger Clarke I, II, III
Professor Peter Croll, I
Mr Keir Dyce I
Mr Sergio Sánchez García I
Professor Justo Carracedo Gallardo I
Mr Muhammad Usman Iqbal II
Professor Margaret Jackson I
Mr Tim Lane I, II
Mr Julian Ligertwood I
Dr Samsung Lim II
Ms Suzanne Lockhart I, III
Mr Mark Loves III
Professor Chris B. Del Mar III
Dr Greg Marston III
Professor Brian Martin II
Mr Carlos González Martínez I
Dr Lauren May I, II
Associate Professor Doug MacKinnon
Dr Katina Michael I, II, III
Dr M.G. Michael I, II, III
Mr George Mickhail II, III
Dr Hasmukh Morarji I
Mr Rob Nicholls II, III
Associate Professor Nicholas O'Brien II, III
Mr Marcus O'Donnell II
Professor Ana Gómez Olivia I
Ms Laura Perusco I
Mr Nigel Phair III
Dr Lucy Resnyansky I, II, III
Dr Mark Rix I, II, III
Associate Professor Greg Rose II
Ms Michelle Rowland II, III
Professor Supriya Singh I
Mr Matthew Sirotich II
Mr James Stellios I
Dr Holly Tootell I, II, III
Mr Adam Trevarthen I
Mr David Vaile III
Mr Jose David Carracedo Verde I
Mr Samuel Fosso Wamba III
Professor Robert Watts III
Professor Marcus Wigan I, II, III

Reviewers

Associate Professor Carole Alcock I, II
Professor Lyn Batten II
Dr Glenn Bewsell III
Dr David Brin II
Professor Simon Bronitt III
Mr Mark Burdon III
Associate Professor L Jean Camp II
Professor Joan Cooper I, III
Dr Karin Garrety II
Associate Professor Sandy Gordon I
Dr Nadirsyah Hosen II
Mr Luke Howie III
Professor Michael Humphrey II
Associate Professor Peter Hyland I, II, III
Professor Margaret Jackson III
Adjunct Professor Don Lamberton II
Professor Stéphane Leman-Langlois II
Mr Julian Ligertwood II
Mr Murray Long II, III
Professor David Lyon II
Professor Brian Martin III
Mr Glen Mattocks II, III
Dr Lauren May III
Adjunct Professor Adrian McCullagh I
Ms Nicola McGarrity III
Dr Katina Michael I, II, III
Dr M.G. Michael I, II, III
Assistant Professor Christine Perakslis II
Dr Vidyasagar Potdar II
Professor Bill Russell III
Professor Jennifer Seberry II
Professor Jill Slay II, III
Dr Holly Tootell III
Dr Ping Yu III

Keywords List (2006-2008)

The keywords below are taken from the papers in the proceedings between the years 2006 and 2008; the bracketed number indicates the frequency of that keyword.

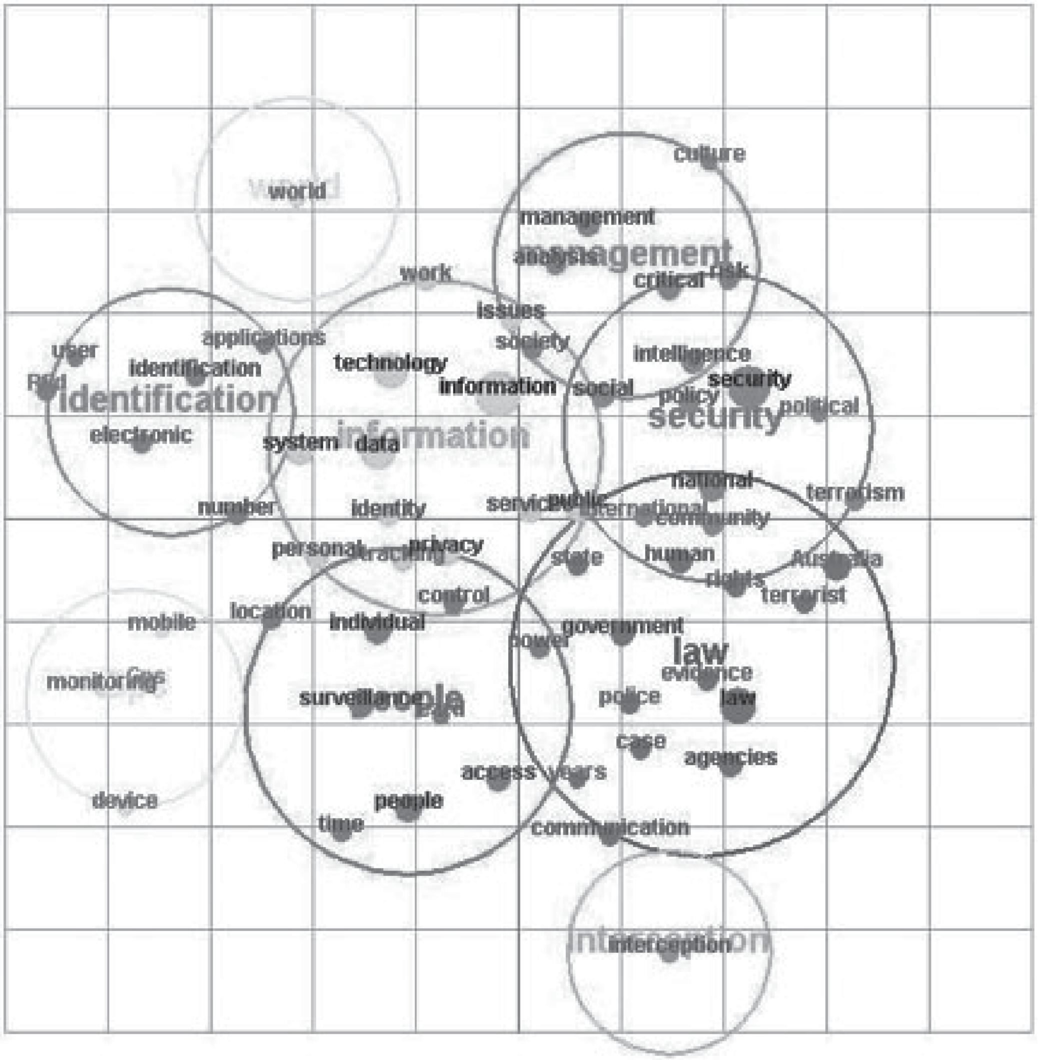
accountability (2), ACTA, adoption and diffusion, AFP, agora, anonymity (3), anti-terrorism legislation (2), apocalyptic, area surveillance, ASIO, assistance to law enforcement agencies,Australian universities, automatic identification (2), best practices, biometrics (3), business intelligence, carbon budget, CBRN, centralised systems, chilling effect, citizen rights (3), civil liberties, client relations, commercialization, community, community legal sector, community perception, compliance, content analysis, contestability, counterveillance principles, courtroom technology, covert surveillance, credentials, criminalization, critical infrastructure (3), critical infrastructure protection (3), critical reflexive approach, critical social theory, culture of compliance, data, data access, data linkage, data management, data-mining, dataveillance (2), DCMA, decision making (3), detention, deterrence, due process, E911, e-courts, e-democracy, efficiency, e-government (2), electronic health data, electronic toll, embedded identity, emergency management, enforcement, enterprise risk management, ePassport, ethics, evaluation methodology, evidence, evidence based policy (3), evidence-based practice, forensic aesthetics, freedom of speech, freight, geospatial, global positioning systems (3), government (2), hand over interface, hazards, history, homeland security, human rights (3), human tracking, identification, identity (3), identity card (2), identity fraud, information (2), information access, Information and Communications Technologies (2), information model, information ownership and consent, information privacy (3), information security (2), information security management, information standards, information systems research, instant message, intellectual property, intelligence (4), intelligence cycle, Intelligent Transport Systems (ITS), interception, interdisciplinary, internal consultancy model, internet, Internet banking, inter-state police cooperation, investigation, IT professionals, justice, knowledge, laboratory, law (3), law enforcement (3), lawful interception (2), legislation, legitimacy, liberty, livestock, location (2), location based services, location privacy, location tracking, location-based services (4), mass murder, mass surveillance, microchip implants, middleware, misanthropy, misology, mobile alerting, mobile telecommunication, modeling (2), mutual legal assistance, myth, national identification, national security (7), national security state, nuclear weapons, object surveillance, omni-surveillance, opposition, organisational culture, outrage, ownership, pan-electron, passport, perceived risk, performance measurement, pervasive technologies, pnyx, policies (2), policy making, politics (2), power (3), practice, privacy (10), privacy impact assessment (PIA), professional identity, profiling, protocols, public data (4), public sector information (PSI), radio-frequency identification (6), real-time business intelligence, reasonable assistance, resistance, retrospective, risk assessment, risk intelligence (2), risk management, risks (3), rule of law, scenario planning, scenarios, Schengen Information System, security (8), security and liberty of the person, security and privacy, security convergence, security framework (2), security management (2), security mechanisms, smart card (2), small to medium enterprise, SMS, social attitudes, social constructivist approach, social impacts (2), social implications, social informatics (2), social networking, social space, sociology of science, speed, state power, stored communication, strategic planning, surveillance (12), suspected terrorists, tactics, telecommunications interception, telematic platform, terrorism (6), testing, theory, threat (4), threat, total farm management, traceability, tracking (2), traffic, transparency, transport, trust (3), überveillance, user acceptance, users' perspective, value chain model, value network model, value workshop model, values, war on terror (2), warrants, weapons of mass destruction, wire tap, wireless network vulnerability assessments

Collaborative Opportunities

Telecommunications Interception and the Law	Simon Bronitt, James Stellios, Rob Nicholls, Michelle Rowland, Katina Michael, Greg Rose, Muhammad Usman Iqbal, Samsung Lim, Marcus Wigan, Roger Clarke, Murray Long, Adrian McCullagh
Power and Information	Brian Martin, Mark Burdon, Steven Clarke, George Mickhail, Roba Abbas, Joan Cooper, Carole Alcock, Stéphane Leman-Langlois
Risk, Intelligence, Security	Mark Loves, Lauren May, Tim Lane, Katina Michael, Mary Barrett, Karin Garrety, Nick O'Brien, Peter Croll, Hasmukh Morarji, Lucy Resnyansky, Jill Slay
Access Card and the Law	Julian Ligertwood, Margaret Jackson, Steven Clark, David Vaile, Roger Clarke
Methodologies	Lucy Resnyansky, Holly Tootell, Laura Perusco, Don Lamberton
Evidence Based Policy	Greg Marston, Rob Watts, Chris Del Mar, Marcus Wigan
Auto-ID Technologies	Katina Michael, Adam Trevarthen, Laura Perusco, Angelo Friggieri, Matt Sirotich, Suzanne Lockhart, Samuel Fosso Wamba, Supriya Singh, Vidyasagar Potdar
Human Rights and Social Implications	Mark Rix, MG Michael, Katina Michael, Marcus O'Donnell, Brian Martin, Michael Humphrey, Nicola McGarrity, Nadirsyah Hosen
Location-Based Services	Marcus Wigan, Katina Michael, Roger Clarke, MG Michael, Muhammad Usman Iqbal, Samsung Lim, Rob Nicholls, Michelle Rowland, Anas Aloudat, L Jean Camp
Policing and Crime Prevention	Nick O'Brien, Doug MacKinnon, Mark Loves, Nigel Phair, Sandy Gordon
Privacy and Surveillance	David Vaile, Roger Clarke, Marcus Wigan, Katina Michael, MG Michael, Holly Tootell, David Lyon, David Brin
Information Security	Lyn Batten, Jennifer Seberry, Karin Garrety, Nigel Phair, Glen Mattocks, Mary Barrett, Lauren May, Ping Yu
Trust	Glenn Bewsell, Nigel Phair, Roger Clarke
Chip Implants	Christine Perakslis, Katina Michael, MG Michael, Holly Tootell

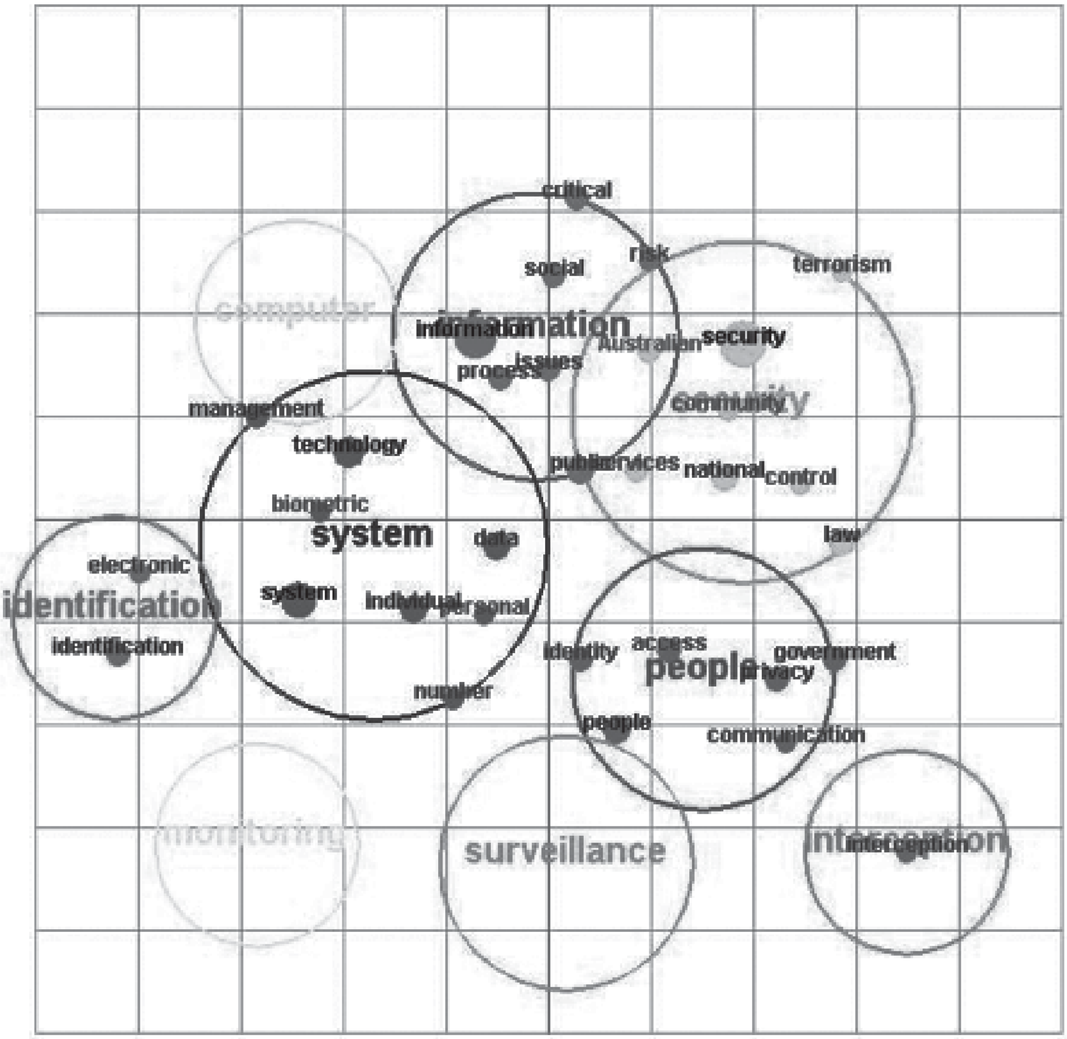
2006-2008 Workshops: Content Analysis Map

(2006) Vol. I The Social Implications of Information Security Measures on Citizens and Business
(2007) Vol. II From Dataveillance to Überveillance and the Realpolitik of the Transparent Society
(2008) Vol. III Australia and the New Technologies: Evidence Based Policy in Public Administration



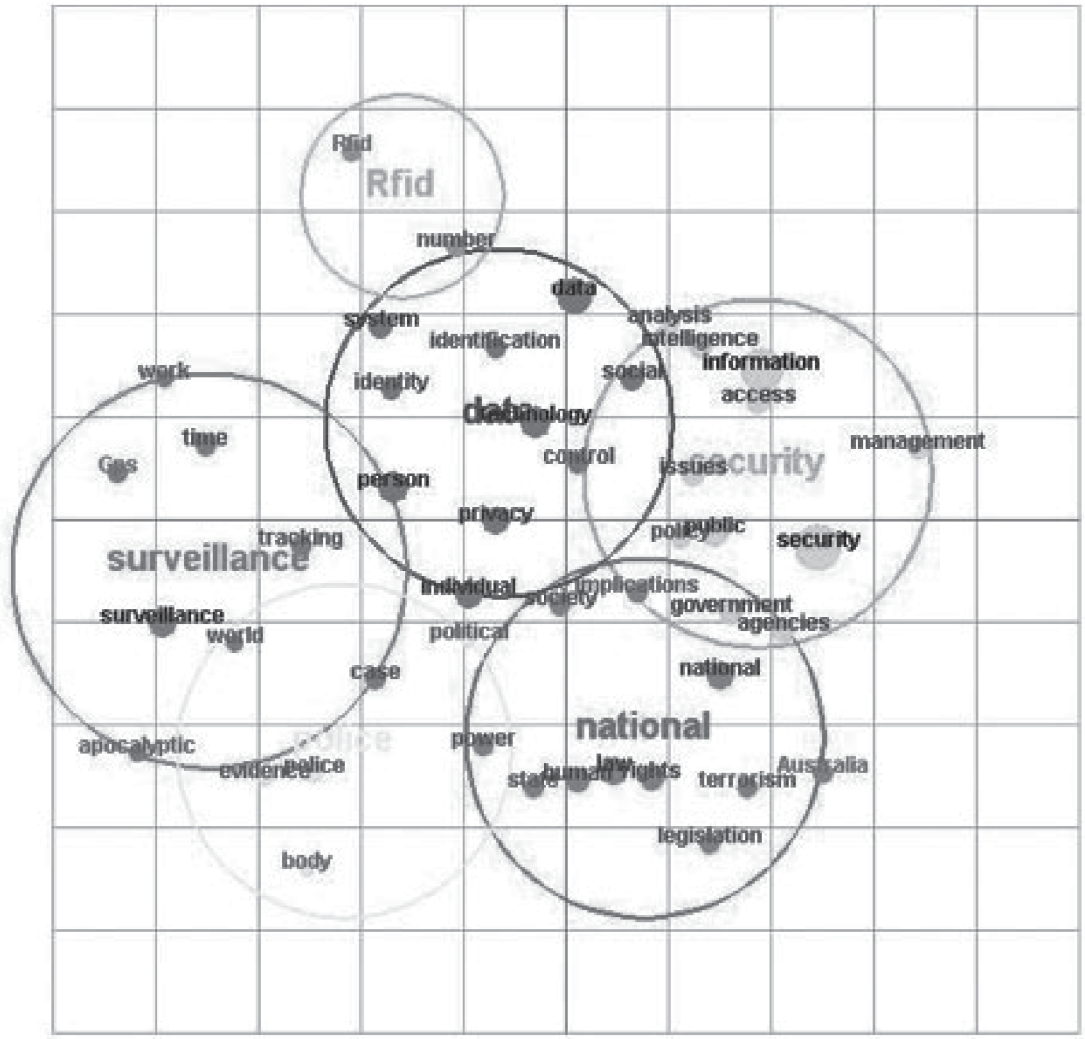
Workshop 2006: Content Analysis

Vol. I The Social Implications of Information Security Measures on Citizens and Business, ISBN 978-1-74128-118-7



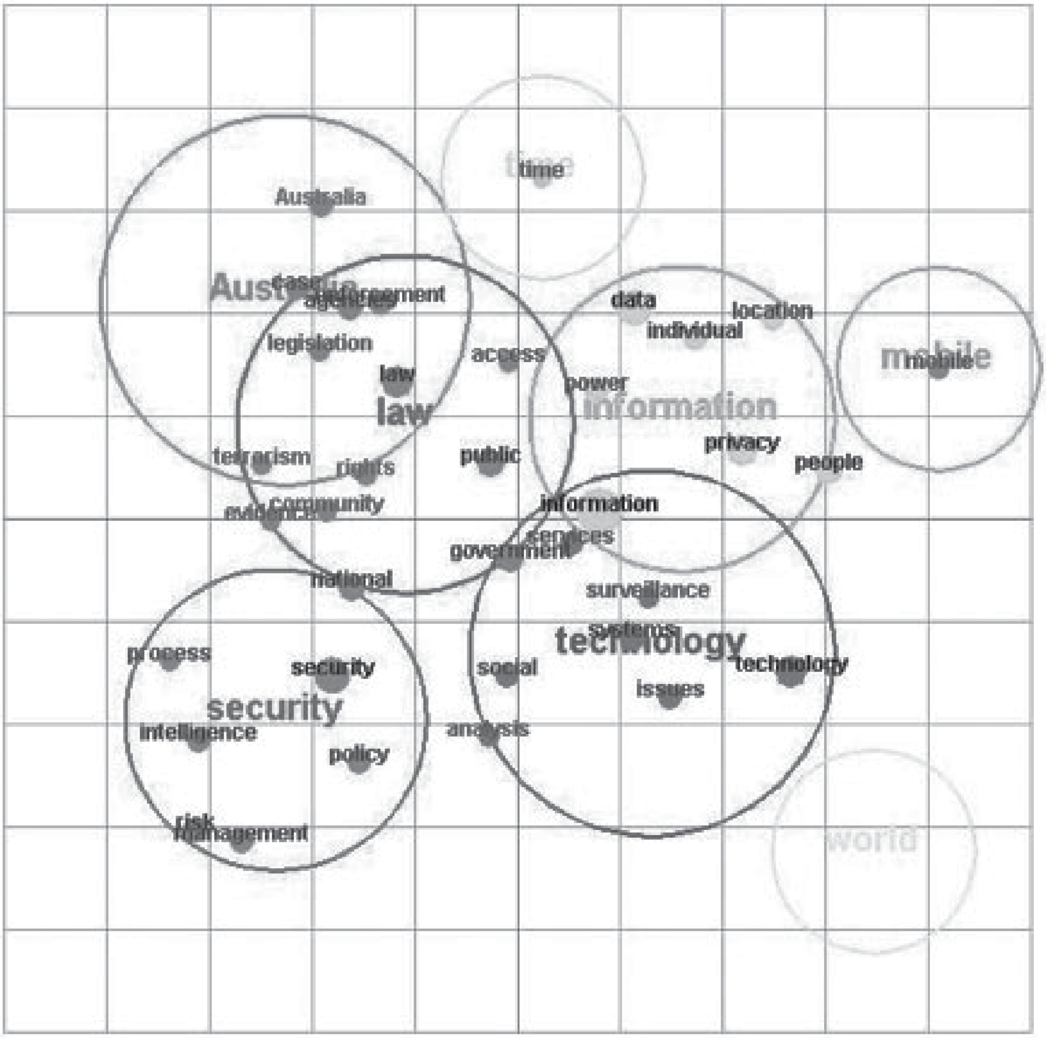
Workshop 2007: Content Analysis

Vol. II From Dataveillance to Überveillance and the Realpolitik of the Transparent Society, ISBN 978-1-74128-141-5



Workshop 2008: Content Analysis

Vol. III Australia and the New Technologies: Evidence Based Policy in Public Administration, ISBN 978-1-74128-150-7



RNSA

Research Network
Secure Australia

The methods of EBP can be transferred to questions of national security usefully, providing some quantitative estimates of the relative benefits or harms of interventions to confront serious threats to Australian national security. It is astonishing such techniques are not used more frequently at the point of decision-making.

Chris Del Mar, Bond University

The current enthusiasm for what is called 'evidence-based policy' may doubtless be explained by advocates for what can variously be called a 'sociology of knowledge' or a 'politics of knowledge'. While there is value in pursuing that kind of reflexive critique, there is arguably value in also exploring in a more fundamental way the relationship between politics, policy and theory/knowledge.

Robert Watts, RMIT & Greg Marston, University of Queensland

The worlds of political spin-doctoring and "intelligence" should be kept clearly separate; hundreds of thousands of ex-Iraqis can explain why. There are nasty local precedents emerging where this separation has broken down, and breathlessly over-stated claims that open-ended surveillance is essential or even effective for improving overall 'security' of the population have been uncritically allowed to undermine the balance between oppressive and increasingly unaccountable 'law enforcement/ national security' powers, and the rights and expectations of citizens to the rule of law which had been hard-won over centuries of contested legal evolution.

David Vaile, University of New South Wales

Any government has an unenviable task in deciding what counter-terrorism legislation to introduce in the case of a massive loss of life. It will be important to ensure that legislation is not born of a knee-jerk reaction to a tragic situation. It should be thoughtful and considered with a 'sunset clause' to ensure that it is reviewed.

Nick O'Brien, Charles Sturt University

This multidisciplinary workshop presents the current and potential status of information security measures, considers their implications on citizens and business, and identifies their impact on legislation and privacy at a local and global level.