



The Second Workshop on the Social Implications of National Security

From Dataveillance to Überveillance and the Realpolitik of the Transparent Society

29 October 2007

Wollongong, 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
Administrator:	Mr. Anant Gupta, University of Melbourne
Node Leader:	Prof Joseph Lai, UNSW@ADFA
Node Leader:	Prof Ed Dawson, Queensland University of Technology
Outreach Manager:	Athol Yates

University of Wollongong



Editors: Michael, K. and Michael, M.G.

Publication Title: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society (Workshop on the Social Implications of National Security, 2007)

Series: Research Network for a Secure Australia (RNSA)

Publisher: University of Wollongong, IP Location-Based Services Research Program (Faculty of Informatics) jointly with the Centre for Transnational Crime Prevention (Faculty of Law)

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/rnsa07.htm>

Publication Year: 2007

Format: Book (hardcopy \$50 AUD; softcopy \$30 AUD <http://www.homelandsecurity.org.au/publications.html>)

Cover and text layout: Anthony Petre

ISBN: 978-1-74128-141-5 (print)

ISBN: 978-1-74128-142-2 (pdf)

All rights reserved. Other than abstracts, no part of this publication may be produced in any form without the written consent of the publisher. The publisher makes no representation or warranty regarding the accuracy, timeliness, suitability or any other aspect of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Foreword

The 2007 Workshop on the *Social Implications of National Security: from Dataveillance to Überveillance and the Realpolitik of the Transparent Society* was organised by the Research Network for a Secure Australia (RNSA) funded by the Australian Research Council. The Workshop will become a biennial event bringing together both researchers and practitioners in the fields relating to the national research priority entitled Safeguarding Australia. In 2007, the workshop was held on the 29th October, at the Function Centre at the University of Wollongong between 8.30 am and 5.00 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.

It provided a forum for the exchange of ideas and research findings between core groups or individuals interested in the social implications of national security measures, focused on the big picture question of Surveillance vs Security.

Workshop participants will learn about the current and potential status of information security measures. The notion of Dataveillance and that of Überveillance are contrasted in the context of national security. What is the price of security that citizens are prepared to pay? Will surveillance technology force us to choose between our right to privacy and national security? This workshop delves deeper into some of the pressing issues facing technology innovation and adoption, government policy, and the legal and regulatory framework.

The cross-disciplinary workshop was seeking perspectives which covered a diverse array of interest areas such as security, information technology, law, philosophy, sociology, religion, politics, history, culture, science and technology studies, and business.

The workshop included papers by Associate Professor of Counter-Terrorism Nicholas O'Brien, Professor of Social Sciences Brian Martin, Professeur des Universités Invité Université d'Orleans George Mickhail, Associate Professor of Law Gregory Rose and Professor of Transport Systems Marcus Wigan. Other professionals presenting include Professor Roger Clarke Principal of Xamax Consultancy (keynote), Mr Rob Nicholls and Ms Michelle Rowland lawyers who work with Gilbert + Tobin, Dr Lucy Resnyansky a research scientist with the Defence Science and Technology Office, and the Information Security Institute's Dr Lauren May.

The Workshop Proceedings contains only peer reviewed papers. The acceptance rate was 63%. Each paper was subjected to a rigorous review process conducted by at least two experts in the appropriate field. The authors were requested to revise the papers according to reviewer's comments. In addition, the editors provided extensive comments for each paper.

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 2nd *Social Implications of National Security* Workshop, the Chair received feedback from the following RNSA members.

Associate Professor Priyan Mendis
Mr Athol Yates
Mr Anant Gupta

We would also like to acknowledge the support of the Dean of the Faculty of Informatics Professor Joe Chicharo, the Director of the Centre for Transnational Crime Prevention Associate Professor Doug MacKinnon, 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-Chair: Holly Tootell
Co-Editor: Dr MG Michael

Reviewers

The editors would like to thank the following reviewers for their assistance in maintaining the high quality of papers.

Associate Professor Carole Alcock	<i>Computer & Information Science, University of South Australia</i>
Professor Lyn Batten	<i>Director of Information Security Group, Deakin University</i>
Dr David Brin	<i>Scientist and Author, Holocene Limited</i>
Associate Professor L Jean Camp	<i>Centre for Applied Cybersecurity Research, Indiana University</i>
Dr Karin Garretty	<i>Senior Lecturer, Faculty of Commerce, University of Wollongong</i>
Dr Nadirsyah Hosen	<i>Lecturer, Faculty of Law, University of Wollongong</i>
Professor Michael Humphrey	<i>Department of Sociology & Social Policy, University of Sydney</i>
Associate Professor Peter Hyland	<i>Head of SISAT, University of Wollongong</i>
Adjunct Professor Don Lamberton	<i>Creative Industries, Queensland University of Technology</i>
Professor Stéphane Leman-Langlois	<i>School of Criminology, University of Montreal</i>
Mr Julian Ligertwood	<i>Research Fellow, Faculty of Law, RMIT University</i>
Mr Murray Long	<i>President, Murray Long & Associates Inc., Ottawa, Ontario, Canada</i>
Professor David Lyon	<i>Killam Research Fellow, Queens Research Chair, Queens University</i>
Mr Glen Mattocks	<i>Private Consultant, Visor Consulting, Canberra, Australia</i>
Dr M.G. Michael	<i>Honorary Fellow, Faculty of Informatics, University of Wollongong</i>
Dr Katina Michael	<i>Senior Lecturer, Faculty of Informatics, University of Wollongong</i>
Assistant Professor Christine Perakslis	<i>The Hospitality College, Johnson & Wales University</i>
Dr Vidyasagar Potdar	<i>Digital Ecosystems and Business Intelligence, Curtin Business School</i>
Professor Jennifer Seberry	<i>Centre for Computer Security Research, University of Wollongong</i>
Associate Professor Jill Slay	<i>Director Forensic Computing Lab, University of South Australia</i>

Table of Contents

1	Opening remarks	7
	<i>Doug MacKinnon</i> <i>Centre for Transnational Crime Prevention, University of Wollongong</i>	
2	A note on überveillance	9
	<i>M.G. Michael and K. Michael</i> <i>School of Information Systems and Technology, University of Wollongong</i>	
3	Keynote address: What 'überveillance' is and what to do about it	27
	<i>Roger Clarke</i> <i>Xamax Consultancy Pty Ltd</i>	
4	Keynote appendix: Surveillance vignettes	47
	<i>Roger Clarke</i> <i>Xamax Consultancy Pty Ltd</i>	
5	Owning identity- one or many- do we have a choice?	61
	<i>Marcus Wigan</i> <i>Oxford Systematics</i>	
6	Opposing surveillance	71
	<i>Brian Martin</i> <i>School of Social Sciences, Media and Communication, University of Wollongong</i>	
7	Message in a bottle: Stored communications interception as practised in Australia	83
	<i>Rob Nicholls and Michelle Rowland</i> <i>Gilbert + Tobin</i>	
8	Australia and the 'war against terrorism': Terrorism, national security and human rights.....	97
	<i>Mark Rix</i> <i>Graduate School of Business, University of Wollongong</i>	
9	Panel session: The case for detention without charge in suspected terrorism cases in Australia ..	113
	<i>Nicholas O'Brien</i> <i>Australian Graduate School of Policing, Charles Sturt University</i>	
10	The benefits and concerns of public data availability in Australia: a survey of security experts	117
	<i>Roba Abbas</i> <i>School of Information Systems and Technology, University of Wollongong</i>	

11	Re-using public sector information (PSI) for profit: Who's data is it anyway?	129
	<i>Mark Burdon</i>	
	<i>Faculty of Law, Queensland University of Technology</i>	
12	The Internet as a communication medium and a social space: a social constructivist approach to the use of open data	147
	<i>Lucy Resnyansky</i>	
	<i>Defence Science and Technology Organisation</i>	
13	The Agora-Pnyx paradox	169
	<i>George Mickhail</i>	
	<i>School of Accounting and Finance, University of Wollongong</i>	
14	Something smart going on: the apocalyptic aesthetics of surveillance	181
	<i>Marcus O'Donnell</i>	
	<i>School of Journalism and Creative Writing, University of Wollongong</i>	
15	Auto-ID and location-based services in national security: Social implications...	201
	<i>Holly Tootell</i>	
	<i>School of Information Systems and Technology, University of Wollongong</i>	
16	Privacy implications of automated GPS tracking and profiling	225
	<i>Muhammad Usman Iqbal and Samsung Lim</i>	
	<i>School of Surveying and Spatial Information Systems, University of New South Wales</i>	
17	Human tracking technology in mutual legal assistance and police inter-state cooperation in international crimes.....	241
	<i>Katina Michael and Gregory Rose</i>	
	<i>School of Information Systems and Technology and Centre for Transnational Crime Prevention, University of Wollongong</i>	
18	ePassport security under the microscope.....	257
	<i>Matthew Sirotich</i>	
	<i>School of Information Systems and Technology, University of Wollongong</i>	
19	Improving information security management: an Australian universities case study	281
	<i>Tim Lane and Lauren May</i>	
	<i>Faculty of Information Technology, Queensland University of Technology</i>	
	Author Biographies	300

1

Opening remarks

Doug MacKinnon

Director, Centre for Transnational Crime Prevention, Faculty of Law,
University of Wollongong

Good morning all.

My name is Doug MacKinnon, I am the director of the Centre for Transnational Crime Prevention at the University of Wollongong. It is a great pleasure to welcome you to this one day workshop entitled: “From Dataveillance to Überveillance and the Realpolitik of the Transparent Society”. This is the second workshop on the *Social Implications of National Security* sponsored by the Research Network for a Secure Australia (RNSA). This workshop will focus on the challenging question of Surveillance vs Security.

In an age, when for all intents and purposes, an apparently normal individual with family and social connections will rise in the morning, say goodbye to his spouse and child and several hours later detonate a suicide bomb in a public place causing death and destruction, many challenges now confront society and those charged with maintaining security, stability and community safety.

Indeed the use of common technology such as mobile phones, by persons of ill intent to coordinate- and on occasions to trigger- catastrophic events now strikes hard at the balance between privacy and the common good.

The issue of balance between privacy and the common good is not a new one to the legal profession and indeed to policymakers, however, historical argument about concepts of public interest versus private needs are challenged by unprecedented threats to civilians and non-combatants by those pursuing political agendas by violent means.

This has recently been demonstrated in Australia through an investigation in Queensland linked to the recent London and Glasgow terrorist strikes. Not only was the Australian legal framework tested but so were new laws and legal processes. In

an era where those charged with the protection of society are indeed often judged by their ability to prevent crime from taking place, law enforcement personnel often find themselves caught in the middle of opposing forces. Ultimately, many would say that the Queensland incident was a true test of the Australian legal system of justice, others might say otherwise, and only time will tell.

For those engaged in social policy and the benefits and disadvantages of technology to society, the examination of the Realpolitik of dataveillance and überveillance need to be considered in the context of national security. Will real or imagined threats lead to a significant increase in surveillance technology and impact on our way of life? Will the balance between privacy and national security change dramatically? The importance of this workshop as it delves deeper into critical factors associated with technology innovation and adoption, government policy, and the legal and regulatory framework, cannot be understated.

The presenters of this workshop come from diverse backgrounds including: legal firms, government agencies, academic institutions across Australia, and some individuals from the business sector. There are papers on stored communications interception and the law, terrorism and human rights, public data versus data protection, location based services and privacy, and ePassports and security.

To the delegates, we hope you enjoy this year's workshop and thank you for coming from all over Australia to be present with us today. It promises to be a day full of challenging issues, learning, and constructive dialogue.

Thank you.

2

A Note on ‘Überveillance’

M.G. Michael¹ and Katina Michael²

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

Abstract

The following note from the editors presents a summary of the term *überveillance*, as it was originally presented by the primary author in May 2006. *Überveillance* is an *above* and *beyond*, an *exaggerated*, an almost omnipresent 24/7 electronic surveillance. It is a surveillance that is not only “always on” but “always with you” (it is *ubiquitous*) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that *omnipresence* in the ‘material’ world will not always equate with *omniscience*, hence the real concern for misinformation, misinterpretation, and information manipulation.

Keywords: surveillance, dataveillance, überveillance, radio-frequency identification (RFID), microchip implants, social implications

1 Überveillance- an emerging concept

Überveillance is an emerging concept, in the full sense of both its application and power it is not yet arrived (M.G. Michael 2007). For some time Roger Clarke's (1988, p. 498) *dataveillance* has been prevalent: the "systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons". Almost twenty years on, technology has developed so much and the national security context has altered so greatly (Snow 2005), that there was a pressing need to formulate a new term to convey both this present reality, and the *Realpolitik* (policy primarily based on power) of our times. It should be said, however, that if it had not been for dataveillance, überveillance could not be. And for that matter, it must be emphasized that dataveillance will always be- it will provide the scorecard for the engine being used to fulfill überveillance.

Überveillance takes that which was "static" or "discrete" in the dataveillance world, and makes it "constant" and "embedded". Consider it not only "automatic" and to do with "identification" BUT also about "location"- that is, the ability to automatically locate AND identify- in essence the ability to perform *automatic location identification* (ALI). It has to do with the fundamental "who" (ID), "where" (location), "when" (time) questions in an attempt to derive "why" (motivation), "what" (result), and even "how" (method/plan/thought). Überveillance can be a predictive mechanism for one's expected behaviour, traits, characteristics, likes or dislikes; or it can be based on historical fact, or something in between. The inherent problem with überveillance is that facts do not always add up to *truth* (ie as in the case of an exclusive disjunction $T+T=F$), and predictions based on intelligence are not always correct.

Überveillance is more than closed circuit television (CCTV) feeds, or cross-agency databases linked to national identity cards, or biometrics and ePassports used for international travel. Überveillance is the sum total of all these types of surveillance and the deliberate integration of an individual's personal data for the continuous tracking and monitoring of identity and location in real time. In its ultimate form, überveillance has to do with more than automatic identification technologies that we carry with us. It has to do with "under the skin" technology that is embedded in the body like microchip implants; it is that which cuts into the flesh- a charagma ("mark"). Think of it as Big Brother, on the inside looking out. This charagma is virtually meaningless without the hybrid network architecture which supports its functionality: to make the person a walking online node, beyond luggable mobile phones, PDAs and smart cards. We are referring here, to the lowest common denominator, the smallest unit of tracking- presently a tiny chip in the body of a human being.

Implants cannot be left behind, cannot be lost, 'cannot' be tampered with, they are always on, can link to objects, make the person seemingly otherworldly. This act of *chipification* is best illustrated by the ever-increasing uses of implant devices for medical prosthesis and for diagnostics (Swedberg 2007). Humancentric

implants are giving rise to the *Electrophorus* (Michael & Michael 2007, p. 313), the bearer of electric technology; an individual entity very different to the sci-fi notion of *Cyborg* as portrayed in such popular television series as the *Six Million Dollar Man* (1974–1978). In its current state the *Electrophorus* relies on a device being triggered wirelessly when it enters an electromagnetic field; these properties now mean that “systems” can interact with people within a spatial dimension, and for the greater part unobtrusively. And it is surely not simple coincidence that alongside *überveillance* we are witnessing the philosophical reawakening (throughout most of the fundamental streams running through our culture) of Nietzsche’s *Übermensch*—the overcoming of the “all-too-human” (Honderich 1995b).

That we might establish that chip implants are not mere science-fiction we need to identify a number of sources which add confirmation to the current reality. It is important to do so because the widespread misconception by information and communication technology (ICT) and engineering researchers at international conferences attended by both authors, is that chip implants are not commercially available for a variety of applications, and that the technology is not relevant to national security *per se*. Some researchers even believe that RFID implants have naught to do with “tracking” and can only be used for “identification”. The following accounts and background sources should place things into perspective, at least at an overview level (see also, K. Michael 2007).

In March of 2005 the European Group on Ethics (EGE) in Science and New Technologies, established by the European Commission (EC), submitted an Opinion on ICT implants in the human body (Rodotà & Capurro 2005). The thirty-four page document outlines a number of legal and ethical issues to do with ICT implants and is premised around the European Union Treaty (Article 6) which has to do with the “fundamental rights” of the individual. Fundamental rights have to do with human dignity, the right to the integrity of the person, and the protection of personal data. From the legal perspective the following was ascertained (Rodotà & Capurro 2005, pp. 18–19):

- a) the existence of a recognised serious but uncertain risk, currently applying to the simplest types of ICT implant in the human body, requires application of the precautionary principle. In particular, one should distinguish between active and passive implants, reversible and irreversible implants, and between offline and online implants;
- b) the purpose *specification principle* mandates at least a distinction between medical and non-medical applications. However, medical applications should also be evaluated stringently and selectively, partly to prevent them from being invoked as a means to legitimise other types of application;
- c) the *data minimisation principle* rules out the lawfulness of ICT implants that are only aimed at identifying patients, if they can be replaced by

- less invasive and equally secure tools;
- d) the *proportionality principle* rules out the lawfulness of implants such as those that are used, for instance, exclusively to facilitate entrance to public premises;
- e) the *principle of integrity and inviolability of the body* rules out that the data subject's consent is sufficient to allow all kinds of implant to be deployed; and
- f) the *dignity principle* prohibits transformation of the body into an object that can be manipulated and controlled remotely – into a mere source of information.

The conclusion is that ICT implants for non-medical purposes violate fundamental legal principles. From the ethical perspective, ICT implants have numerous issues, including the requirement for: non-instrumentalisation, privacy, non-discrimination, informed consent, equity, and the precautionary principle (see also IEEE 2007; Lewan 2007a; Burton and Stockhausen 2005). It should be stated, however, that the EGE while not recommending ICT implants for non-medical applications because they are fundamentally fraught with legal and ethical issues, did state the following (Rodotà & Capurro 2005, p. 32):

ICT implants for surveillance in particular threaten human dignity. They could be used by state authorities, individuals and groups to increase their power over others. The implants could be used to locate people (and also to retrieve other kinds of information about them). This might be justified for security reasons (early release for prisoners) or for safety reasons (location of vulnerable children).

However, the EGE insists that such surveillance applications of ICT implants may only be permitted if the legislator considers that there is an urgent and justified necessity in a democratic society (Article 8 of the Human Rights Convention) and there are no less intrusive methods. Nevertheless the EGE does not favour such uses and considers that surveillance applications, under all circumstances, must be specified in legislation. Surveillance procedures in individual cases should be approved and monitored by an independent court.

The same general principles should apply to the use of ICT implants for military purposes.

Although this Opinion was entirely comprehensive for its time, we hold growing concerns for the development of the information society, the lack of public debate and awareness regarding this emerging technology, and the pressing need for regulation that has not eventuated commensurate to developments in this domain.

Herein rests the problem of human rights and the “balance” between freedom, security and justice. First, it is a built-in fallacy to speak of a balance. In the microchip implant scenario, there will never be a balance, so long as someone else has the potential to control the implant device or the stored data about us which is linked to

the device. Second, we are living in a period where chip implants for the purposes of *segregation* are being discussed seriously by health officials and politicians. We are speaking here of the identification of groups of people in the name of “health management” or “national security.” We will almost certainly witness new, and more fixed forms, of ‘electronic’ apartheid. Whatever the guise of parliamentary speak we are not far from such potentially explosive perils as a global community.

Consider the very real case where the “Papua Legislative Council is deliberating a regulation that would see microchips implanted in people living with HIV/AIDS so authorities could monitor their actions” (Somba 2007). Similar discussions on “registration” were held regarding asylum seekers and illegal immigrants in the European Union (Hawthorne 2001). RFID implants or the “tagging” of populations in Asia (eg Singapore) were also considered “the next step” in the containment and eradication of the Severe Acute Respiratory Syndrome (SARS) in 2003 before it subsided (RFID 2003). Apart from disease outbreaks, RFID has also been discussed as a response and recovery device for emergency services personnel dispatched to terrorist disasters (BBC 2005), and for the identification of victims of natural disasters, such as in the case of the Boxing Day Tsunami (Channel 2005). The question remains whether there is a truly legitimate use function of chip implants for the purposes of emergency management as opposed to other applications. ‘Definition’ plays a critical role in this instance. A similar debate has ensued in the use and application of the Schengen Information System (SIS) II in the European Union where differing states have recorded alerts on individuals based on their definition and understanding of “security risk” (Guild and Bigo 2002).

In June of 2006, legislative analyst, Anthony Gad, reported in brief 06-13 for the *Legislative Reference Bureau*, that:

2005 Wisconsin Act 482, passed by the legislature and signed by Governor Jim Doyle on May 30, 2006, prohibits the required implanting of microchips in humans. It is the first law of its kind in the nation reflecting a proactive attempt to prevent potential abuses of this emergent technology.

Today a number of states in the United States have passed similar laws, despite the fact that the U.S. Food and Drug Administration (FDA, 2004) at the national level have allowed radio frequency identification implants for medical use in humans. The Wisconsin Act (2006) states:

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows: SECTION 1. 146.25 of the statutes is created to read: 146.25 Required implanting of microchip prohibited. (1) No person may require an individual to undergo the implanting of a microchip. (2) Any person who violates sub. (1) may be required to forfeit not more than \$10,000. Each day of continued violation constitutes a separate offense.

North Dakota was the next state to follow Wisconsin’s example. Governor John

Hoeven signed a two sentence bill into state legislature on 4 April 2007. The bill was criticised by some who said that while it protected citizens from being “injected” with an implant, it did not prevent someone from making them swallow it (Songini 2007). More recently, Californian Governor Arnold Schwarzenegger, signed bill SB 362 proposed by state Senator Joe Simitian barring “employers and others from forcing people to have a radio frequency identification (RFID) device implanted under their skin” (Woolfolk 2007; Jones 2007). According to the Californian Office of Privacy Protection (2007) this bill

...would prohibit a person from requiring any other individual to undergo the subcutaneous implanting of an identification device. It would allow an aggrieved party to bring an action against a violator for injunctive relief or for the assessment of civil penalties to be determined by the court.

The bill which will be effective 1 January 2008, did not receive support from the technology industry on the contention that it was “unnecessary”.

Interestingly, however, it is in the United States, that most chip implant applications have come to pass despite the calls for caution. This is not surprising given the first human-implantable passive RFID microchip (the VeriChip™) was approved for medical use in October of 2004 by the U.S. Food and Drug Administration. Today the VeriChip Corporation has 900 hospitals across the United States that have registered the VeriMed system, and now the corporation’s focus has moved to “patient enrollment” including people with diabetes, Alzheimer’s and dementia (Diabetes News 2007). The VeriMed™ Patient Identification System is used for “rapidly and accurately identifying people who arrive in an emergency room and are unable to communicate” (VeriChip 2007).

In July of 2006 (The Age, 2007), CityWatcher.com reported two of its employees had “glass encapsulated microchips with miniature antennas embedded in their forearms... merely a way of restricting access to vaults that held sensitive data and images for police departments, a layer of security beyond key cards and clearance codes.” It is not difficult to see how implants may soon find themselves being applied to the corrective services sector (RFID 2006). In 2002, 27 of 50 American states were using some form of satellite surveillance to monitor parolees. Similar schemes have been used in Sweden since 1994. In the majority of cases, parolees wear wireless wrist or ankle bracelets and carry small boxes containing the vital tracking and positioning technology. The positioning transmitter emits a constant signal that is monitored at a central intelligence point (Michael & Masters 2006a). Despite continued claims by researchers that RFID is only used for identification purposes, *Health Data Management* (2005a) disclosed that VeriChip (the primary commercial RFID implant patient ID provider) had enhanced its patient wander application by adding the ability to follow the “real-time location of patients, the ability to define containment areas for different classes of patients, and one-touch alerting. The system now also features the ability to track equipment in addition to

patients.” A number of these issues have moved the American Medical Association to produce an ethics code for RFID chip implants. Due to copyright restrictions, we cannot quote this code here but it can be sourced online (Sade 2007; Reichman 2006; Bacheldor 2007).

In chip implant cases outside the U.S. we also find a number of diverse applications for humancentric RFID. VeriChip’s Scott Silverman had stated in 2004 that 7,000 chip implants had been given to distributors of which it was estimated 1,000 chips had been implanted in humans by year end worldwide (Weissert 2004). Today the number of VeriChip implantees is estimated to be at about 2,000. So where did all these chips go? Well, they may not be mainstream applications, but they are in operation. As far back as 2004, a nightclub in Barcelona, Spain, the *VIP Baja Beach Club* in Catalan City (Chase 2007) was offering “its VIP clients the opportunity to have a syringe-injected microchip implanted in their upper arms that not only [gave] them special access to VIP lounges, but also [acted] as a debit account from which they [could] pay for drinks” (Morton 2004). Microchips have also been implanted in 160 Mexican officials in the law enforcement sector (Weissert 2004). “Mexico’s top federal prosecutors and investigators began receiving chip implants in their arms... in order to get access to restricted areas inside the attorney general’s headquarters.” In this instance, the implant acted as an access control security device despite the documented evidence purporting to the fact that RFID is not a secure technology at all (see *Gartner Research* report by Reynolds 2004).

In the United Kingdom, *The Guardian* (Wilson 2002), reported that 11-year old Danielle Duval had an active chip (i.e. containing a rechargeable battery) implanted in her. Her mother believes that it is no different to tracking a stolen car, simply that it is being used for another more important application. Mrs Duvall is considering implanting her younger daughter age 7 as well but will wait until the child is a bit older, “so that she fully understands what’s happening”. In Tokyo, Japan, the Kyowa Corporation in 2004 manufactured a schoolbag with a GPS device fitted into it, to meet parental concerns about crime, and in 2005 Yokohama City children were involved in a four month RFID bracelet trial using the I-Safety system (Swedberg 2005). In 2007, we now have a company in Lancashire in England, Trutex, which is seriously considering fitting the school uniforms they manufacture with RFID (Meikle 2007). What might be next? Concerned parents enforce microchip implants on minors?

More recently decade-old experimental studies on microchip implants in rats have come to light tying the device to tumours (Lewan, 2007b). The American Veterinary Medical Association (AVMA 2007) was so concerned with the report that on 13 September 2007 they released the following statement, quoted here in full:

The American Veterinary Medical Association (AVMA) is very concerned about recent reports and studies that have linked microchip identification implants, commonly used in dogs and cats, to cancer in

dogs and laboratory animals. AVMA staff and member veterinarians are actively looking into any potential for this technology to induce tumor formation in dogs, cats, or people but must await more definitive data and test results before taking further action. Based on the fact that a large number of pets have already been implanted with this microchip technology and there has been a relatively small number of confirmed cases of chip-induced tumors, the AVMA advises pet owners against a rush to judgment on the technology. In fact, there is a concern among veterinary medical researchers that some of the research into chip-induced tumors may be flawed, because the animals used were genetically predisposed to cancer. In addition, **removal of the chip is a more invasive procedure and not without potential complications**. It's clear that there is a need for more scientific research into this technology. [bold eds.]

We can see here, already, evidence pointing to the notion of 'no return'—an admittance that removal of the chip is not easy, and not without complications.

Let us for a moment revisit the decade old case of the Norplant System, the *levonorgestrel* contraceptive inserts that over 1 million women in the United States, and over 3.6 million women worldwide had been implanted with through 1996 (AMA 1997). The implants were inserted just under the skin of the upper arm in a surgical procedure under local anesthesia and could be removed in a similar fashion. As of 1997, there were 2,700 Norplant suits pending in the state and federal courts across the United States alone. Most of the claims had to do with "pain or damage associated with insertion or removal of the implants... [p]laintiffs have contended that they were not adequately warned, however, concerning the degree or severity of these events" (AMA 1997). While the Norplant system did not use RFID there are many lessons to be gained. Concerns for the potential for widespread health implications caused by human-centric implants have also been around for some time, it should not surprise us. In 2003, Covacio provided evidence why implants may impact humans adversely, categorizing these into thermal (i.e. whole/partial rise in body heating), stimulation (i.e. excitation of nerves and muscles) and other effects most of which are currently unknown.

The future is here now, and it is *wireless*. What is not completely here yet are the formal service level agreements to hand-off transactions between different types of networks owned by a multitude of network providers (few of whom are truly global)—free or commercial. These architectures and protocols are being developed, and it is only a matter of time before existing technologies have the capability to track individuals between indoor and outdoor locations seamlessly, or a new technology is created to do what present-day networks cannot (Identec 2007). For instance, a wristwatch device with GPS capabilities to be worn under the skin translucently is one idea that was proposed as far back as 1998. Hengartner and Steenkiste (2005)

forewarn that “[l]ocation is a sensitive piece of information” and that “releasing it to random entities might pose security and privacy risks.”

In short, there is *nowhere* to hide in this digital society, and *nothing* remains private (in due course, perhaps, not even our thoughts). *Nanotechnology*, the engineering of functional systems at the molecular level, is also set to change the way we perceive surveillance– microscopic bugs (some 50,000 times smaller than the width of the human hair) will be more parasitic than even the most advanced silicon-based *auto-ID* technologies. In the future we may be wearing hundreds of microscopic implants, each relating to an exomuscle or an exoskeleton, and which have the power to interact with literally millions of objects in the ‘outside world’. The dangers are not whether state governments will invest in this technology, they are and they will (Ratner & Ratner 2004), but whether the next generation will idealistically view this technology as super ‘cool’ and ‘convenient’ and opt-in without comprehending the full extent of their compliance.

The social implications of these *über*-intrusive technologies will have no restricted limits or political borders. They will affect everything from our day-to-day existence, to our family and community relations. They will give rise to mental health problems, even more complex forms of paranoia and obsessive compulsive disorder. The refusal of some thinkers to admit to a body and mind correlation, i.e. psychophysical interaction, is progressively losing ground with many now agreeing, especially with the support of modern neuroscience, that “the intimate relation between bodily and psychic functions is basic to our personal identity” (Rodotà and Capurro 2005, p. 3). Even those engaged in religious observances will be affected, especially in the context of their practice of confession and their specific understanding of absolution of ‘sin’– we might ‘confess’ as much as we might want, but the records on the database, ‘the slate’, will not be wiped ‘clean’. The list of social implications is endless; it is an exercise for our imaginations. Whatever our respective *-ism* or not, condition of our mental health or not, this ‘peeping Tom’ which we will carry on the inside, will have manifest consequences for that which philosophers and theologians normally term *self-consciousness*.

In all of this rest the multiple paradoxical levels of *über*veillance. In the first instance, it will be one of the great blunders of the new political order to think that chip implants (or indeed nanodevices) will provide the last inch of detail required to know where a person is, what they are doing, and what they are thinking. Authentic ambient *context* will always be lacking, and this will further aggravate the potential ‘puppeteers’ of any comprehensive surveillance system. Marcus Wigan captures this critical facet of “context” very well in his paper where he speaks of “asymmetric information” held by third parties. Second, chip implants will not necessarily make you smarter or more aware (unless you can *afford* it, of course), but on the contrary and under the ‘right’ circumstances make us increasingly dumb and mute. Third, chip implants are not the panacea they are made out to be– they can fail, they can be stolen, they are not tamper-proof, and they may cause harmful effects to the

body- they are after all a foreign object and their primary function is to relate to the outside world not the body itself (as in the case of pacemakers and cochlear implants). Fourth, chip implants in our present framework in any case, do not give you greater control over your space, but allow for others to control you and to decrease your autonomy and as a result your interpersonal trust at both societal and state levels. *Trust* is inexorably linked to both *metaphysical* and *moral* freedom. Therefore the naive position routinely heard in the public domain that if you have “nothing to hide, why worry?” misses the point entirely. Fifth, chip implants will create a presently unimaginable digital divide- we are not referring to computer access here, or Internet access, but access to another mode of existence. The “haves” (implantees) and the “have-nots” (non-implantees) will not be on speaking terms; perhaps a fresh interpretive approach to the biblical account of the tower of Babel (Gen. 11:9).

At this point of adoption, unless the implant is removed within a short time, the body will adopt the foreign object and tie it to tissue. At this moment, there will be no exit strategy, no contingency plan, it will be a life enslaved to upgrades, virus protection mechanisms, and inescapable intrusion. Imagine a working situation where your computer- the one which has all your personal data stored on it- has been hit by a worm, and becomes increasingly inoperable and subject to overflow errors and connectivity problems, being the only machine you could use; now imagine the same thing happening with an embedded implant. There would be *little* choice other than to upgrade or, the unthinkable, to opt out of the networked world altogether.

The first discernible movement towards this escalating and forward-looking scenario, with the potential to entangle us all “both small and great”, will be our unique and ‘non-refundable’ identification number (ID). The universal drive to provide us all with cradle-to-grave ULIs (unique lifetime identifiers) which will replace our names is gaining increasing momentum, especially post *September 11*. Philosophers have generally held that our names are the most identifiable expressions of our personhood. Names, they have argued, are the signification of identity and origin; our names possess both sense and reference (Honderich 1995a, 602f). Two of the twentieth century’s greatest political consciousness (one who survived the Stalinist purges and the other the holocaust) Aleksandr Solzhenitsyn and Primo Levi, have warned us of the connection between murderous regimes and the numbering of individuals. There is no quicker way to dehumanize an individual than by ‘removing’ someone’s name and replacing it with a number. It is far easier to extinguish an individual on every level if you are ‘rubbing’ out a number rather than a life history.

Aleksandr Solzhenitsyn recounts in one place from his famous anti-Stalinist testament, *The Gulag Archipelago* (1918-56), (2007, p. 346f):

Then again, they [Corrective Labor Camps] quite blatantly borrowed

from the Nazis a practice which had proved valuable to them – the substitution of a number for the prisoner’s name, his “I”, his human individuality, so that the difference between one man and another was a digit more or less in an otherwise identical row of figures... [i]f you remember all this, it may not surprise you to hear that making him wear numbers was the most hurtful and effective way of damaging a prisoner’s self-respect.

Primo Levi writes similarly in his own well-known account of the human condition in *The Drowned and the Saved* (1989, p. 94f):

Altogether different is what must be said about the tattoo [the number], an altogether autochthonous Auschwitzian invention... [t]he operation was not very painful and lasted no more than a minute, but it was traumatic. Its symbolic meaning was clear to everyone: this is an indelible mark, you will never leave here; this is the mark with which slaves are branded and cattle sent to the slaughter, and this is what you have become. You no longer have a name; this is your new name.

And many centuries before both Solzhenitsyn and Levi were to become acknowledged as two of the greatest political consciences of our times, an exile on the isle of Patmos– during the reign of the Emperor Domitian– expressed a disturbingly comparable position when referring to the abuses of the *emperor cult* which was especially practiced in Asia Minor away from the more sophisticated population of Rome (M.G. Michael 1998, pp. 176–196). He was Saint John the Evangelist, commonly recognized as the author of the *Revelation* (c. A.D. 95):

He causes all, both small and great, rich and poor, free and slave, to receive a mark on their hand or on their foreheads, and that no one may buy or sell except one who has the mark or the name of the beast, or the number of his name. Here is wisdom. Let him who has understanding calculate the number of the beast, for it is the number of a man: His number is 666 (Rev 13:16–18).

The technological infrastructures: the software, the middleware, and the hardware for ULIs, are readily available to support a diverse range of humancentric applications, and increasingly those embedded technologies which will eventually support überveillance. Multi-national corporations, particularly those involved in telecommunications and banking, are investing millions (expecting literally billions in return) in such ‘identifiable’ technologies that have a tracking capability. At the same time the media which in most instances can yield more sway with people than government institutions themselves, squanders this influence and is not intelligently challenging this auto-ID (automatic identification) trajectory. As if in chorus, blockbuster productions from Hollywood are playing up all forms of *biometrics* as not only hip and smart, but also as *unavoidable* mini-device fashion accessories for the upwardly mobile, and attractive. Advertising, of course, plays a dominant role in

this cultural *tech-rap*. Advertisers are well aware that the market is literally limitless and demographically accessible at all levels (and more tantalizingly from cradle-to-grave consumers). Our culture, which in previous generations was for the better part the van guard against most things detrimental to our collective well-being, is dangerously close to bankrupt (it already is *idol worshipping*) and has progressively become fecund territory for whatever idiocy might take our fancy. Carl Bernstein (1992) of Bernstein and Woodward fame has captured the atmosphere of recent times very well:

We are in the process of creating what deserves to be called the idiot culture. Not an idiot sub-culture, which every society has bubbling beneath the surface and which can provide harmless fun; but the culture itself. For the first time the weird and the stupid and the coarse are becoming our cultural norm, even our cultural ideal.

Oddly enough, given this technological fixation with which most of the world is engaged, there is a perceptible mood of a collective disquiet that something is not as it should be. In the face of that, this self-deception of ‘wellness’ is not only taking a stronger hold on us, but it is also being rationalized and deconstructed on many authoritative platforms and levels. We must break free of this dangerous daydream to make out the cracks that have already started to appear on the gold tinted rim of this seeming 21st century utopia. The *machine*, the new technicized “gulag archipelago” is ever pitiless and without conscience. It can tear sinew; crush bones; break spirits; and rip out hearts without ever needing to take a break.

Lest there be any misunderstanding the authors of this note are not anti-government, after all, the alternative is anarchy-; nor are they conspiracy theorists (though we now know better than to rule out *all* conspiracy theories). Nor do they believe that these dark scenarios need necessarily eventuate as precisely as they are describing them. But they do believe that we are close to reaching the critical point of no return. Others believe that point is much closer (ACLU, 2007). It remains for individuals to speak up and argue for, and to demand regulation, as has happened in several states in the United States where Acts have been established to avoid *microchipping* without an individual’s consent, i.e. compulsory electronic tagging of citizens. Our politicians (there are some exceptions) for a number of reasons will not legislate on this issue of their own accord, it would involve multifaceted industry and absorb too much of their time, and the fear they might be labelled anti-technology or worse still, failing to do all that they can in the fight against “terror”. This is one of the components of the modern-day Realpolitik which in its push for the *transparent society* is bulldozing ahead without any true sensibility for the richness, fullness, and sensitivity of the undergrowth. As an actively engaged community, as a body of concerned researchers with an ecumenical conscience and voice, we can make a difference by postponing or even downgrading the doomsday scenario of even the most pessimistic futurist.

Finally, the editors would like to underscore two main points. First, the positions, projections, and beliefs expressed in this summary do not necessarily reflect the positions, projections, and beliefs of the individual contributors to this volume. And second, as with our previous workshop, it is clear that the authors of the papers do embrace all that which is vital and dynamic with technology, but reject its rampant application and diffusion without studied consideration as to the potential effects and consequences.

References

- ACLU (2007). "Surveillance Society Clock 23:54", *American Civil Liberties Union*, <<http://www.aclu.org/privacy/spying/surveillancesocietyclock.html>> (Accessed 5 October 2007).
- AMA (1997). "Norplant System Contraceptive Inserts", *Report 9 of the Council on Scientific Affairs (I-97)*, *American Medical Association*, <<http://www.ama-assn.org/ama/pub/category/print/13593.html>> Accessed 5 October 2007.
- AVMA (13 September 2007). "Breaking News: Statement on Microchipping", *American Veterinary Medical Association*, <http://www.avma.org/aa/microchip/breaking_news_070913_pf.asp> Accessed 5 October 2007.
- Bacheldor, B. (17 July 2007). "AMA Issues Ethics Code for RFID Chip Implants", *RFID Journal*, <<http://www.rfidjournal.com/article/articleprint/3487/-1/1/>> Accessed 4 October 2007.
- Ball, E. and Bond, K. (2005). "Bess Marion v. Eddie Cafka and ECC Enterprises, Inc., No. 2005-CV-0237", *IT Moot Court*, <<http://www.itmootcourt.com/2005%20Briefs/Petitioner/Team18.pdf>> Accessed 2 October 2007.
- BBC. (28 July 2005). "Implant Chip to Identify the Dead", *BBC News*, <<http://news.bbc.co.uk/1/hi/technology/4721175.stm>> Accessed 10 January 2006.
- Bernstein, C. (1992). *The Guardian*, June 3.
- Burton, P. and Stockhausen, K. (22 February 2005). *The Australian Medical Association's Submission to the Legal and Constitutional's Inquiry into the Privacy Act 1988* <[http://www.ama.com.au/web.nsf/doc/WEEN-69X6DV/\\$file/Privacy_Submission_to_Senate_Committee.doc](http://www.ama.com.au/web.nsf/doc/WEEN-69X6DV/$file/Privacy_Submission_to_Senate_Committee.doc)> Accessed 5 October 2007.
- Californian Office of Privacy Protection. (23 July 2007). "California Privacy Legislation", *Office of Privacy Protection, State of California*, <<http://www.privacy.ca.gov/califlegis.htm>> Accessed 10 October 2007.
- Channel (3 January 2005). "Thai Wave Disaster Largest Forensic Challenge In Years: Expert", *Channel News Asia*, <http://www.channelnewsasia.com/stories/afp_asiapacific/view/125459/1/.html> Accessed 10 February 2005.
- Chase, C. (n.d.). VIP Verichip, *Baja Beach House- Zona VIP*, <<http://www.baja-beachclub.com/bajaes/asp/zonavip2.aspx>> Accessed 12 October 2007.
- Clarke, R.A. (1988). "Information Technology and Dataveillance", *Communications of the ACM*, 31(5), pp. 498-512.
- Covacio, S. (2003). "Technological Problems Associated with the Subcutaneous

- Microchips for Human Identification (SMHId), *InSITE- "Where Parallels Intersect*, June, pp. 843-853.
- Diabetes News. (20 March 2007). "13 Diabetics Implanted With VeriMed RFID Microchip At Boston Diabetes EXPO", *Medical News Today*, <<http://www.medicalnewstoday.com/articles/65560.php>> Accessed 9 October 2007.
- FDA (10 December 2004). "Medical Devices; General Hospital and Personal Use Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information", *U.S. Food and Drug Administration- Department of Health and Human Services*, 69(237), <<http://www.fda.gov/ohrms/dockets/98fr/04-27077.htm>> 5 October 2007.
- Gad, A. (June 2006). "Legislative Brief 06-13: Human Microchip Implantation", *Legislative Briefs from the Legislative Reference Bureau*, <<http://www.legis.state.wi.us/lrb/pubs/Lb/06Lb13.pdf>> 5 October 2007.
- Guild, E. and Bigo, D. (2002). "The Schengen Border System and Enlargement" in Malcolm Anderson and Joanna Apap (eds), *Police and Justice Co-operation and the New European Borders*, European Monographs, pp. 121-138.
- Hawthorne, M. (13 December 2001). "Refugees Meeting Hears Proposal To Register Every Human In The World", *Sydney Morning Herald*, <<http://www.smh.com.au/breaking/2001/12/14/FFX058CU6VC.html>> Accessed 1 July 2003.
- HDM. (May 2005a). "VeriChip Enhances Patient Wander App", *Health Data Management*, <<http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12361>> Accessed 5 October 2007.
- HDM (July 2005b). "VeriChip Buys Monitoring Tech Vendor", *Health Data Management*, <<http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12458>> Accessed 5 October 2007.
- HDM. (October 2005c). "Chips Keep Tabs on Babies, Moms", *Health Data Management*, <<http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=15439>> Accessed 5 October 2007.
- HDM. (July 2007). "Baylor Uses RFID to Track Newborns", *Health Data Management*, <<http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=15439>> Accessed 5 October 2007.
- Hengartner, U. and Steenkiste, P. (2005). "Access Control to People Location Information", *ACM Transactions on Information and System Security*, 8(4), pp. 424-456.
- Honderich, T. (ed.) (1995a). "Names" in *Oxford Companion to Philosophy*, Oxford University Press, Oxford, p. 602f.
- Honderich, T. (ed.) (1995b). "Nietzsche, Friedrich" in *Oxford Companion to Philosophy*, Oxford University Press, Oxford, p. 619-623.
- Identech (2007). "RFID Tags Equipped with GPS", *Navigadget*, <<http://www.navigadget.com/index.php/2007/06/27/rfid-tags-equipped-with-gps/>> Accessed 10 October 2007.

- IEEE (March 2007), "Me & My RFIDs", *IEEE Spectrum*, 4(3) 2007, pp. 14-25.
- Jones, K.C. (4 September 2007). "California Passes Bill To Ban Forced RFID Tagging", *InformationWeek*, <<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201803861>> Accessed 10 October 2007.
- Lewan, T. (2007a) "Microchips Implanted in Humans: High-Tech Helpers, or Big Brother's Surveillance Tools?" *The Associated Press*, <<http://abcnews.go.com/print?id=3401306>> Accessed 5 October 2007.
- Lewan, T. (9 September 2007b). "Chip Implants Linked to Animal Tumors", *Associated Press/ WashingtonPost.com*, <<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/09/AR2007090900467.html>> Accessed 4 October 2007.
- Meikle, J. (21 August 2007). "Pupils Face Tracking Bugs in School Blazers", *The Guardian*, <http://www.guardian.co.uk/uk_news/story/0,2152979,00.html> Accessed 24 August 2007.
- Michael, K. (2007). "Selected Works of Dr. Katina Michael", *University of Wollongong*, <<http://ro.uow.edu.au/kmichael/>> Accessed 5 October 2007.
- Michael, K. & Masters, A. (2006a). "Realised Applications of Positioning Technologies in Defense Intelligence" in D. Essam & H. Abbass (eds), *Applications of Information Systems to Homeland Security and Defense*, IDG Press, ch. 7, pp. 164-192.
- Michael, K. & Masters, A. (2006b). "The Advancement of Positioning Technologies in Defence Intelligence" in D. Essam & H. Abbass (eds), *Applications of Information Systems to Homeland Security and Defense*, IDG Press, ch. 8, pp. 193-214.
- Michael, K. & Michael, M.G. (2006). "Towards *chipification*: the multifunctional body art of the net generation", *Cultural Attitudes Towards Technology and Communication*, (28th-1st July: Tartu, Estonia), pp. 622-641.
- Michael, K. & Michael, M.G. (2007). "Homo Electricus and the Continued Speciation of Humans", in Marian Quigley (ed.), *The Encyclopedia of Information Ethics and Security*, IGI Global, pp. 312-318.
- Michael, M.G. (1998). "Ch IX: Imperial Cult" in *The Number of the Beast, 666 (Revelation 13:16-18): Background, Sources, and Interpretation* Unpublished Honors Masters by Research Thesis at Macquarie University, pp. 176-196.
- Michael, M.G. (2007). "Überveillance: 24/7 x 365- People Tracking and Monitoring", *The 29th International Conference of Data Protection and Privacy Commissioners: Privacy Horizons, Terra Incognita*, 25-28 September, Montreal, Canada, <http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html> Accessed 30 September 2007.
- Morton, S. (2004). "Barcelona Clubbers Get Chipped", *BBC News*, <<http://news.bbc.co.uk/2/hi/technology/3697940.stm>> Accessed 11 October 2007.
- Ratner, D & Ratner M.A. (2004). *Nanotechnology and Homeland Security: New Weapons for New Wars*, Prentice Hall, New Jersey.

- Reichman, J. H. (2006). "RFID Labeling in Humans", American Medical Association House of Delegates: Resolution: 6 (A-06), *Reference Committee on Amendments to Constitution and Bylaws* <<http://www.ama-assn.org/ama1/pub/upload/mm/471/006a06.doc>> Accessed 5 October 2007.
- Reynolds, M. (20 July 2004). "Despite the Hype, Microchip Implants Won't Deliver Security", *Gartner Research*, <http://www.gartner.com/DisplayDocument?doc_cd=121944> Accessed 12 October 2007.
- RFID. (4 June 2003). "Singapore Fights SARS with RFID", *RFID Journal*, <<http://www.rfidjournal.com/article/articleprint/446/-1/1/>> Accessed 10 August 2005.
- RFID. (22 August 2006). "I Am Not A Number - Tracking Australian Prisoners With Wearable RFID Tech", *RFID Gazette*, <http://www.rfidgazette.org/2006/08/i_am_not_a_num.html> Accessed 11 October 2007.
- Rodotà, S. and Capurro, R. (16 March 2005). "Ethical Aspects of ICT Implants in the Human Body", *Opinion of the European Group on Ethics in Science and New Technologies to the European Commission N° 20 Adopted on 16/03/2005*, <http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf> Accessed 4 October 2007.
- RNZI (25 July 2007). "Papua Legislative Council Deliberating Microchip Regulation for People With HIV/AIDS", *Radio New Zealand International*, <<http://www.rnzi.com/pages/news.php?op=read&id=33896>> Accessed 12 October 2007.
- Sade, R.M. (2007). "Radio Frequency ID Devices in Humans, Report of the Council on Ethical and Judicial Affairs: CEJA Report 5-A-07" in R.E. Quinn *Reference Committee on Amendments to Constitution and Bylaws* <http://www.ama-assn.org/ama1/pub/upload/mm/369/ceja_5a07.pdf> Accessed 5 October 2007.
- Schuerenberg, B.K. (February 2005a). "Implantable RFID Chip Takes Root in CIO: Beta tester praises new mobile device, though some experts see obstacles to widespread adoption", *Health Data Management*, <<http://www.healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12232>> Accessed 5 October 2007.
- Schuerenberg, B.K. (November 2005b). "Patients Let RFID Get Under Their Skin", *Health Data Management*, <<http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12601>> Accessed 5 October 2007.
- Somba, N.D. (24 July 2007). "Papua Considers 'Chipping' People with HIV/AIDS", *The Jakarta Post*, <<http://www.thejakartapost.com/yesterdaydetail.asp?fileid=20070724.G04>> Accessed 12 October 2007.
- Songini, M.L. (12 April 2007). "N.D. Bans Forced RFID Chipping, Governor Wants a Balance between Technology, Privacy", *ComputerWorld*, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385&intsrc=hm_topic> Accessed 10

- October 2007.
- Snow, D.M. (2005). *National Security For A New Era: Globalization And Geopolitics*, Addison-Wesley.
- Swedberg, C. (16 December 2005). "RFID Watches Over School Kids in Japan", *RFID Journal*, <<http://www.rfidjournal.com/article/articleview/2050/1/1/>> Accessed 11 October 2007.
- Swedberg, C. (25 May 2007). "Alzheimer's Care Center to Carry Out VeriChip Pilot", *RFID Journal*, <<http://www.rfidjournal.com/article/articleview/3340/1/1/>> Accessed 8 October 2007.
- The Age (22 July 2007). "Chips: High Tech Aids or Tracking Tools?" *Fairfax Digital: The Age*, <<http://www.theage.com.au/news/Technology/Microchip-Implants-Raise-Privacy-Concern/2007/07/22/1184560127138.html>> Accessed 4 October 2007.
- Verichip. (11 October 2007). "VeriChip Corporation Adds More Than 200 Hospitals at the American College of Emergency Physicians (ACEP) Conference", *VeriChip News Release* <<http://www.verichipcorp.com/news/1192106879>> Accessed 11 October 2007.
- Weissert, W. (14 July 2004). "Microchips implanted in Mexican officials", *Associated Press*, <<http://www.msnbc.msn.com/id/5439055/>> Accessed 11 October 2007.
- Wilson, J. (2002). "Girl to Get Tracker Implant to Ease Parents' Fears", *The Guardian*, <<http://www.guardian.co.uk/Print/0,3858,4493297,00.html>> Accessed 15 October 2002.
- Wisconsin Act (30 May 2006). "Wisconsin Act 482", <<http://www.legis.state.wi.us/2005/data/acts/05Act482.pdf>> Accessed 4 October 2007.
- Woolfolk, J. (12 October 2007). "Back Off, Boss: Forcible RFID Implants Outlawed in California", *Mercury News*, <http://www.mercurynews.com/portlet/article/html/fragments/print_article.jsp?articleId=7162880&siteId=568> Accessed 13 October 2007.

3

What ‘überveillance’ is and what to do about it

Roger Clarke

Xamax Consultancy Pty Ltd

Visiting Professor at UNSW, ANU and the University of Hong Kong

Abstract

Mere surveillance is passé. The idea was worth discussing as recently as a quarter-century ago, but no longer. Technologists have delivered, and marketers have promoted (and exaggerated), a host of additional capabilities.

A new term that might better describe the current circumstances is ‘überveillance’. This paper provides both a theoretical and an empirical context within which to assess alternative interpretations of that notion. It culminates in a set of Principles whereby the balance that has been lost in recent years can be restored.

Keywords: surveillance, dataveillance, omni-surveillance, pan-electron, Counterveillance Principles

1 Introduction

Corporate marketers have promoted a vast array of technologies as means to monitor the behaviour of all manner of things. Parliaments have suspended their disbelief and permitted government agencies to buy technologies and install systems. Some corporations have imposed similar schemes on their employees, and on their customers.

There is enormous diversity among the schemes that have been installed or proposed. Indeed, there are many objectives, and considerable specialisation is occurring, with the result that surveillance is going through divergence and even splintering.

But there are also signs of convergence and coordination, and this creates both some degree of promise and a vastly increased level of threat to society. The workshop committee has selected ‘überveillance’ as the theme around which the new direction can be examined.

This keynote commences by underlining key aspects of the surveillance notion. It then briefly scans the range of surveillance schemes. The intention is to lay a foundation for a typology of schemes, for comparison and contrast, and ultimately for a critical appreciation of the benefits, disbenefits and risks that are inherent in the process of inter-relating surveillance schemes.

Three alternative interpretations of the notion of ‘überveillance’ are then discussed, translating ‘über’ variously as ‘all’, as ‘exaggerated’ and as ‘supra’. Finally, themes arising from these discussions are developed into a small set of Principles that must be applied in order to avoid the over-reaction to the threat of ‘terrorism’ causing our societies to eat themselves.

2 The fundamentals of ‘surveillance’

The number of different surveillance schemes is so great that a comprehensive survey requires substantial resources. This section commences by re-visiting a couple of key concepts, as a prelude to vignettes of a number of rather different kinds of surveillance.

In my work in this area over the last 20 years, I’ve referred to surveillance as “the systematic investigation or monitoring of the actions or communications of one or more persons”. This requires some adjustment, in particular to take account of the monitoring of spaces, and of objects other than humans. The primary concern of this paper is the surveillance of people and their behaviour, whether directly or indirectly.

The original forms of **physical surveillance** were typified by visual observation, and symbolised by Bentham’s panopticon.

Watching and listening have come to be aided by equipment of various kinds which offers enhancement of optical and aural signals, e.g. through telescopes and directional microphones. This has enabled **physical surveillance at distance**.

A development in recent years has been the emergent phenomenon of what might be called **auto-physical surveillance**. This is enabled by means of devices that are attached to the person (whether loosely but reliably, as with a mobile phone, or tightly as with an anklet, or even embedded). Rather than the modern connotation of 'automated', the prefix 'auto-' is intended here to convey its original meaning of 'self-'.

Progressively, surveillance ceased to be constrained to the observation of ephemera. The recording of signals meant that data trails could be built up, and that **retrospective analysis** could be undertaken of those trails. As the number of such trails increased, information originating from different times and places could be interwoven, enabling additional inferences to be drawn.

The monitoring of data-flows, and the analysis of data-holdings, are economically efficient because they can be automated. Furthermore, they are inherently surreptitious, so the watched are far less aware of the watchers than is the case with physical surveillance, even at distance. As a result, **dataveillance** (a convenient contraction of 'data surveillance') has been used to augment, and increasingly to substitute for, physical surveillance (Clarke 1988). The volume of monitoring undertaken has also grown, because its inexpensiveness enables more of it to be done within the same budget. The natural limitations on the number of men who can be hired to wear trench-coats and watch doorways have been overcome.

As telecommunications improved, a further capability was added. The data became available very shortly after it was collected, which meant that the trail was warm and **real-time tracking** could be conducted. This increased the chances of being able to intercept a target. It also created the possibility of **predictive tracking**, by inferring a target's intended destination.

As telecommunications developed, first telegraphic, then telephonic and later facsimile transmissions became vehicles for **electronic surveillance**. In recent decades, this has been extended to all forms of Internet communications, particularly those that depend on wired connections, but also the various unwired channels.

Until recently, electronic communications supported the equivalent of speech. Generally, the law permitted **connections monitoring or traffic analysis** (who is talking with whom) although it subjected such activities to controls. Because of the enormous intrusiveness and the risks involved in granting powers to law enforcement agencies, much greater obstacles were placed in the way of **communications surveillance** (who is saying what to whom).

Since the advent of the Web in the early-to-mid-1990s, however, electronic communications also support the equivalents of buying books and going to the library. The monitoring being conducted by employers and governments is now far more intrusive, because what might be described as **experience surveillance** provides access not merely to what a person is saying, but also to what they are thinking about and researching.

Within each of the categories discussed above, it is important to distinguish two

sub-categories:

- **personal surveillance.** This is focussed on an identified person, generally for a specific reason. It is undertaken because suspicion has arisen from some other source
- **mass surveillance.** This is far less precisely targeted, and is imposed on groups of people, often large groups. Generally, its purpose is to identify individuals who belong to some particular class of interest to the surveillance organisation. In short, it is a suspicion-generator, designed to produce candidates against whose actions counter-measures or pre-counters can be implemented, or who can be submitted to personal surveillance

Physical surveillance was applied to a **location or place**. Enhancements enabled the watcher and their equipment to be separated by some distance from that place, but the locus of the surveillance remained the same. Three different categories of place have been discernible, which might be described as private, controlled and public.

The notion of **private places** corresponds to locations in which an individual, or two, or perhaps a few, could reasonably expect not to be subject to surveillance by other parties. This has seemed to have a central core of the marital bedroom, a more qualified zone comprising the rest of the home and even more so its visible exterior (gardens and patios), and some further outposts such as the insides of toilet cubicles.

Organisations that exercise substantial control over particular places have asserted the right to conduct surveillance where, when and how they wish. The contestability of claims in relation to **controlled places** increases from, for example, the rooms from which nuclear power stations and air traffic are controlled, via the footpaths outside government agencies and the faces presenting to ATMs, to railway stations and cinema precincts.

One interpretation of **public place** is ‘everywhere that is neither of the other two’. The numerous subscribers to the ‘original sin’ philosophy of life tend to assert that all forms of surveillance of public places are legitimate, on the grounds that privacy inherently doesn’t exist in public places, or no longer exists in public places, or should not exist in public places.

Yet people have always had reasonable expectations of privacy in public places. That applies all the more to people who are not well-known. More generally, people, whether well-known or not, have a reasonable expectation of privacy when they are behaving in a manner that is intended to be private, e.g. when in the company of family, rather than projecting themselves (or their ‘public persona’) to some kind of ‘public’. Because parliaments have been slow to protect such behaviours, the courts are being forced to develop a tort through case law.

Electronic surveillance broke the nexus with a single location. Initially, it was feasible to re-define it to a multi-location phenomenon, as in the monitoring of

both ends of a phone conversation. But first dataveillance and then new forms of electronic surveillance forced further re-thinking. It is now necessary to define the actions or communications that are subject to surveillance as occurring in **‘space’ rather than ‘place’**, and to conceive of the space as being either physical or figurative (as in abstractions such as ‘cyberspace’). With that change, the old concepts of private, controlled and public places have given way to **private, controlled and public spaces**.

The purposes and potential benefits of surveillance are discussed in section 2 of Wigan & Clarke (2006). This paper focusses primarily on its negative impacts.

3 Mini-case studies in surveillance

As an intrinsic part of this presentation, a collection of vignettes was prepared. These describe a wide array of instances of surveillance, with considerable differences in purpose, style and intensity. Partly because of the length of the text and partly in order to make them accessible independently of this paper, they have been presented in an Appendix to this paper (see chapter 4).

4 The categorisation of surveillance

The diversity that is evident in that collection of vignettes suggests the need to be clear about the dimensions across which applications vary. Drawing on the outline of the surveillance concept in section 2 above, the following can be distinguished:

(1) Of What?

That which is subjected to surveillance may be a specified individual, specified groups of individuals, specified objects, specified groups of objects, or a specified space.

(2) For Whom?

The beneficiaries of surveillance may be the individual who is the subject of the surveillance, an individual who has a direct interest in the subject of the surveillance, or another party with an interest in the behaviour of the subject.

(3) By Whom?

The surveillance may be conducted by the individual who is the subject of the surveillance, an individual who has a direct interest in the subject of the surveillance, another party with an interest in the behaviour of the subject, or a third party that is in some sense acting on behalf of one of the above.

(4) Why?

The primary purpose of the surveillance may be to assist with the health or safety of the subject of surveillance, to detect or collect evidence of behaviour that conforms or does not conform with some norm, or to encourage conformant

behaviour and/or deter non-conformant behaviour.

(5) How?

The means whereby the surveillance is conducted may be physical surveillance (visual and aural), physical surveillance at distance, auto-surveillance, retrospective analysis, dataveillance, real-time tracking, predictive tracking, traffic analysis, communications surveillance or experience surveillance; and each of them may be targeted personal surveillance or much broader mass surveillance.

(6) Where?

The locus of the surveillance may be defined in physical space, or in some virtual space. A common form of virtual space is that enabled by electronic communication networks, but another is the web of ideas inherent in published text, uttered words and recorded behaviour.

(7) When?

The timeframe in which surveillance is conducted may be defined across a single span of time, or recurrent spans (such as a particular span within each 24-hour cycle), or scattered across time (e.g. triggered by particular conditions detected in published text, uttered words and recorded behaviour), or continuous and unrelenting.

The public and political acceptability, the legality, and the effectiveness of a particular instance of surveillance differ greatly depending on the design choices that it evidences. An approach to developing an ethical framework for surveillance is in Michael, McNamee & Michael (2006).

5 What is überveillance?

The theme of the workshop originates in the work of the Editors, Michael and Katina Michael, with the first published use in lecture notes (M.G. Michael 2006). The notion is emergent rather than established, and it continues to evolve. A useful working definition that they offer is “an above and beyond omnipresent 24/7 surveillance where the explicit concerns for misinformation, misinterpretation, and information manipulation, are ever more multiplied and where potentially the technology is embedded into our body” (Michael & Michael 2006, p. 361)

In this section, this author approaches the idea afresh, and considers several possible interpretations of the term, including, but not restricted to, the Michael & Michael quotation above.

The word appears not to have existed until Michael & Michael coined it. Its stem and suffix, ‘-veillance’, are clearly co-opted from ‘surveillance’. Originally, this derived from the French ‘surveiller’, whose contemporary senses include ‘to keep an eye on’ (e.g. luggage), to supervise (e.g. people), to monitor (e.g. people, an object or a space), and to invigilate (to watch candidates in an examination).

Judging by the entry in the Oxford English Dictionary, the word was co-

opted into English in 1799, originally in a report on the French Revolution. The relationship was readily recognised with Bentham's panopticon proposal, which originated in 1787 but was current for 25 years. During the 200 years since then, the English word 'surveillance' has come to be used primarily with sinister associations. It has been subject to a number of adaptations and extensions, including this author's own neologism 'dataveillance', of 1988, which the Michaels explicitly identify as one of the inspirations for their own work.

The prefix 'über' is drawn directly from German. Its several senses are investigated in the following sub-sections.

5.1 Omni-Surveillance

An apocalyptic vision would see 'überveillance' as referring to surveillance that applies across all space and all time (omni-present), and support some organisation that is all-seeing and even all-knowing (omniscient), at least relative to some person or object. The apocalyptic theme is a key thread in M.G. Michael's work. See Michael (1998; 2000a; 2000b; 2003).

An effective way to do this would be to embed the surveillance mechanism within the person or thing to be monitored, and endow it with the capacity to monitor itself continuously, and report to a monitoring authority, whether periodically, by exception, or continuously. Applying the dictum that 'information is power', this leads easily to a feeling of inevitability of the surveillance organisation becoming an all-powerful (omnipotent) being.

On the one hand, this is the stuff of science fiction, and the dystopian genre within sci-fi at that. On the other, most of the elements needed to realise the nightmare already exist, including:

- chips with substantial capacity to gather, store, process and output data;
- devices containing such chips that can be reliably associated with individuals (as already occurs consensually with mobile phones, and non-consensually with anklets and wristlets on various categories of the institutionalised, particularly prisoners, parolees and even remandees);
- chips that can be (and, in small quantities already have been) embedded in humans;
- convenient, readily replenishable power sources for such chips (such as that already available when the carrier moves through a magnetic field to induce current in an antenna); and
- wireless networks through which data can be transmitted.

Remarkable as it may seem, some categories of people are being enveigled, coerced and even mandated to submit to such a 'pan-electricon', particularly as a condition of employment, or in return for reduced constraints on the space within which the individual is permitted to move. Aspects of the 'digital persona' in contexts

such as these are investigated in Clarke (2005b).

If the word ‘überveillance’ achieves broad currency, this may well be the primary interpretation that our children and grandchildren have of it. It remains somewhat speculative at this stage, however, and is sufficiently forbidding that many people are likely to remain ‘in denial’. The following two alternative interpretations may therefore be of greater immediate value in investigating the idea and what we need to do about it right now.

5.2 Exaggerated Surveillance

One interpretation of ‘überveillance’ questions the extent to which surveillance is undertaken. This can be along various dimensions, as discussed in section 4 above. For example, surveillance may be excessive because it has too broad a scope, or is instigated for reasons that are minor in comparison with its negative impacts. In either case, its justification is exaggerated.

(1) The Costs and Disbenefits

Surveillance has costs and disbenefits, and its benefits need to be balanced against them. The costs and disbenefits may be incurred by the organisation conducting the surveillance, or by others, particularly the individuals subjected to it.

The term ‘costs’ is used here in the financial sense, and includes all forms of expenditure, in particular on the conduct of the surveillance, on the infrastructure to support it, and on the analysis of the resulting data stream(s). It encompasses at least some of the costs of actions taken as a result of surveillance, in particular those actions that transpire to have been unjustified because they arose from ‘false positives’.

The notion ‘disbenefits’ is used to encompass non-financial impacts that are negative, whether for the society, economy or polity as a whole, or only for some individuals or groups. The enormous scope of disbenefits arising from surveillance is exemplified by the list in Exhibit 1.

Exhibit 1: Real and Potential Dangers of Dataveillance

From Clarke (1988)

Dangers of Personal Dataveillance

- wrong identification
- low quality data
- acontextual use of data
- low quality decisions
- lack of subject knowledge of data flows
- lack of subject consent to, data flows
- blacklisting
- denial of redemption

Dangers of Mass Dataveillance

• To the Individual

- arbitrariness
- acontextual data merger
- complexity and incomprehensibility of data
- witch hunts
- ex-ante discrimination and guilt prediction
- selective advertising
- inversion of the onus of proof
- covert operations
- unknown accusations and accusers
- denial of due process

• To Society

- prevailing climate of suspicion
- adversarial relationships
- focus of law enforcement on easily detectable and provable offences
- inequitable application of the law
- decreased respect for the law and law enforcers
- reduction in the meaningfulness of individual actions
- reduction in self-reliance and self-determination
- stultification of originality
- increased tendency to opt out of the official level of society
- weakening of society's moral fibre and cohesion
- destabilisation of the strategic balance of power
- repressive potential for a totalitarian government

(2) Controls Over Excesses

A crucial question in any organic system is the extent to which natural controls exist. If natural controls are in place and not seriously impeded, then the system may be best left to find its own equilibrium. If, on the other hand, the controls are retarded in a significant way, then some intervention may be needed, in order to overcome the impediments, or to stimulate the control aspects. In some settings, however, the system may be doomed to spiral out of control. In that case, the architecture is in need of overhaul if the system is to survive.

To what extent is surveillance an organic system, and which of those archetypes best describes it?

In Clarke (1995a), ‘intrinsic controls’ over the particular dataveillance technique of data matching were examined. They were found to include:

- the exercise of countervailing political power by the class of data subjects affected by the process, by their representatives, by the mass media, or by the general public. Given the imbalance of power between organisations and individuals, it is not realistic to expect this factor to be of any great significance except in particular circumstances;
- the displeasure of some organisation, such as a competitor or regulatory agency;
- self-restraint practised by the agency itself, influenced by professional norms, or by an appreciation of the delicacy of public confidence in its institutions and the resultant need to respect constitutional rights and moral concerns; and
- general blundering.

That paper concluded that “the intrinsic factor which might be expected to exercise the most significant degree of control over computer matching is economics: surely government agencies will not apply the technique in circumstances in which it is not worthwhile. The primary means whereby the economic factor will influence decision-making about computer matching programs is cost/benefit analysis”. The various forms of cost/benefit analysis are described in Clarke & Stevens (1997) and (Clarke 2007).

A mere decade later, that sentiment seems quaint. In the present decade, government agencies have barely adopted so much as a pretence of conducting cost/benefit analyses. They have become thoroughly politicised, and ‘business cases’ dominate. A ‘business case’ differs from a cost/benefit analysis in two important ways. It is one-dimensional, because it adopts the view of the sponsor, rather than reflecting the varying perspectives of multiple stakeholders. Secondly, it is essentially designed as a justification of a policy position that has already been adopted, rather than as an analytical tool.

In the surveillance arena, there has not only been little evidence of cost/benefit

analysis being applied, there has seldom even been a compelling business case. The proponents of surveillance successfully avoid scrutiny of their proposals, especially since the windfall of the terrorist strikes in New York and Washington DC in 2001, and what marketers refer to as ‘mid-life kickers’ in Bali in 2002, in Madrid in 2004, and in London in 2005. Since 2001, surveillance has been implemented as an imperative, as those worst forms of policy-formation – knee-jerk reaction, bandwagon effect, and sacred cow.

The biometrics industry provides a valuable case study. Most biometrics technologies cannot and do not deliver on their promises, partly because the environments in which they are applied are complex and messy, and partly because most biometrics technologies are technically flawed. It is therefore not in the interests of the providers of technologies and services to provide truthful information or to submit to evaluation.

Surely ‘the truth will out’, user organisations will discover that ‘the emperor has no clothes’, and the mythologies of surveillance will become common knowledge?

Instead, an extraordinary phenomenon has emerged, that has not been evident in other contexts – alliances of vendors and user organisations. The US national security community has contrived the publication of tests and reports that have been quite grossly twisted and biased, in order to provide biometrics vendors with breathing-space, and with credibility that their products do not warrant. The most extreme instance is in the laughably inadequate technology falsely projected as ‘facial recognition’. The Face Recognition Vendor Test (FRVT) projects have been breathtaking in their misrepresentation of reality. They were jointly sponsored by a group including the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST) and the Department of Homeland Security.

In Australia, the corruption has been mirrored in the Biometrics ‘Institute’. This organisation has a grand-sounding name, but its function is to provide a forum for the alignment of organisations whose interests, in an organic system, would be at considerable variance from one another. Government agencies and suppliers have conspired, and continue to conspire, to project biometrics technologies as things that they are not: effective, reliable, and safe for human consumption.

Corporations, unlike governments and government agencies, are subject to the constraints of return on investment (ROI). This somewhat tempers their enthusiasm for monitoring. For these reasons, the financial sector has long resisted strong authentication on its customers. It also appears that the full power of consumer profiling and ‘customer relationship management’ technology may not yet have been unleashed on Australian consumers.

But ROI has proven inadequate to ensure rational designs. The private sector too makes decisions that are far from balanced, because knee-jerk and bandwagon outweigh rationality. In addition, there has been increasing pressure from Governments, using such ‘motherhood and apple pie’ sentiments as ‘money-laundering’, ‘counter-terrorism’, ‘homeland’ and ‘critical infrastructure protection’.

The 2006-07 rounds of 'Anti-Money-Laundering and Counter-Terrorism Financing' (AML-CTF) legislation represent one of the most extreme forms of exaggeration to date, with business enterprises now obligatorily enlisted as spies against their customers.

5.3 Master-Surveillance

Another possible interpretation of 'überveillance' derives from the use of 'über' to imply 'meta', 'supra' or 'master'-surveillance.

This could involve the **consolidation** of multiple surveillance threads in order to develop what would be envisaged by its proponents to be superior information. This might be performed *ad hoc*, as occurs in 'intelligence assessment' agencies active in foreign affairs and national security.

The challenges are enormous, however. In particular, the data-flows are typically highly variable and highly unreliable. The bases on which they are conceived and implemented vary greatly between the streams. There may be very considerable differences between the aims of each individual operator and the would-be 'master'. The challenges of diversity in data sources, data meaning and data quality were investigated in the context of data matching programs in Clarke (1995b).

In order to overcome the difficulties inherent in consolidating very different streams of information, there could be endeavours to achieve **coordination** among the various surveillance sources. An example of such an approach is the creation of an organisation whose express purpose is to draw surveillance organisations closer together. A prime example was the creation of the U.S. Department of Homeland Security (which in the process changed the sense of 'DHS' from Human Services to something differently protective and much more sinister).

An approach that might seem superior to both consolidation and coordination is **centralisation**. This involves the conception of an architecture intended from the outset to develop a set of feeds into a single 'master', with all of the subsidiary surveillance processes serving the centrally-determined objectives. Stafford Beer naively thought that a centrally-planned cyber-economy could be consistent with an open society and a democratic polity. The experience of Beer's Cybersyn project (1970-73) could have delivered the *coup de grace* to such Promethean idealism if Chile had not been seen to be acting against the interests of the American way of profit. Its elected President was eliminated, and with him Beer's experiment.

During the 1970s and 1980s, such 'central planning' approaches were derided. To some extent this was due to their totalitarian nature, demanding as they do a controlled and inherently static society. But the primary reason was that they had been demonstrated not only behind the Iron Curtain, in Cuba and under East Asian Communist regimes, but also in France, to lead to economic systems that were ineffective, inefficient and in most cases downright stagnant.

Up to a point, systems generally exhibit efficiencies of scale, and efficiencies of scope. Beyond that point, they become unwieldy, excessively complex, and

inherently unmanageable. Systems of the complexity of societies are well beyond the flex-point. They accordingly exhibit substantial inefficiencies of scale and of scope. General systems theory recognises that, for large-scale systems to have the flexibility and adaptability that they need for survival, they need to comprise loosely coupled elements, and to be subject to control through the interplay of those elements rather than through any form of centrally-determined control.

6 What do we do about überveillance?

The picture painted in the preceding sections may seem bleak. Surveillance is rampant. Human values have been trampled. Osama bin Laden and Al Qaeda, or rather the effigies that have been made of them, have triumphed. The limited and sporadic attacks in their names have struck at the moral weaknesses and contradictions inherent in the ‘Western’, ‘democratic’ world. That world has turned inwards on itself. It is spiralling towards self-destruction through the denial of the very freedoms on which it was supposed to be built. Our world needs an antidote to ‘national security extremism’, and it needs it fast.

This section distills a few key messages about what we need to do in order to ensure survival of society, the economy and the polity, in the face of rampant ‘control freaks’. It enunciates a small set of Principles that will contribute to the restoration of Australian society by bringing the surveillance mania back under control. The intention is to generate countervailing power against the extremism of the national security agencies. In this context, a variant of the label ‘countervallance’ to ‘counterveillance’ is appropriate. Exhibit 2 lists the Principles, and the remainder of the section provides brief descriptions of them.

Exhibit 2: Counterveillance Principles

1. Independent Evaluation of Technology
2. A Moratorium on Technology Deployments
3. Open Information Flows
4. Justification for Proposed Measures
5. Consultation and Participation
6. Evaluation
7. Design Principles
 1. Balance
 2. Independent Controls
 3. Nymity and Multiple Identity
8. Rollback

The position adopted in developing these Principles is not itself extremist. It is common ground across society that terrorists are killing people from time to time, that there are (small numbers of) disaffected individuals who will be attracted to violent ‘solutions’, that religious fundamentalism is a threat to open societies, that

countermeasures are needed, and that both general alertness and capable public security institutions are needed.

Where this set of Principles might be seen by some to be radical is in the following:

- it recognises that terrorism is not new and nor is it unusual
- although the ‘power to weight ratio’ of a single strike has increased (because fewer terrorists can deliver a bigger payload), it denies that this has particularly significant implications for public policy
- it refuses to accept reactionary extremism at face value, and to provide national security and law enforcement interests with *carte blanche* to do what they say needs to be done in order to counter the threats
- it denies that ‘secrecy’ is a necessary pre-condition of ‘security’
- it rejects the legitimacy of treating what are really ‘public safety’ issues as though they were ‘national security’ matters
- it is deeply sceptical about counter-terrorism depending on everyone having to be limited to a single State-managed identity, because this helps not at all against ‘virgin terrorists’

(1) Independent Evaluation of Technology

Surveillance of the intensive kinds that are drastically altering our society are heavily dependent on technologies. The assertions of technologists and marketers must be viewed with scepticism, and subjected to testing. That testing must not be warped, and must not be conducted by participants in the field of play (such as the FBI, NSA, NIST, and, in Australia, the Defence Science & Technology Organisation – DSTO). Normal science and technology must be resumed. Rather than ‘Government policy’ driving and twisting outcomes, rational consideration of technologies and their applications is essential.

(2) A Moratorium on Technology Deployments

Some years ago, I called for a moratorium on biometric implementations in Australia (Clarke 2003). I did not do so idly. I argued that “[a] ban must be imposed on the application of biometrics technologies until and unless a comprehensive and legally enforced regulatory regime has been established”. My rationale was not only that applications of biometrics had quite gross, negative impacts, but also that a moratorium might well be the only means of saving an industry that has promised much for years and delivered very little.

There are enormous impediments to the adoption of ‘advanced technologies’. In the majority of cases, their dysfunctions are considerable, and the extent to which they achieve their primary objectives is in serious doubt. The identification and authentication schemes for the APEC meeting in Sydney were as much of a farce

as the traffic control system that let The Chasers' convoy through beyond the point of embarrassment.

(3) Open Information Flows

The antidote to inappropriate deployments of inadequate technologies is openness. The public needs facts about the context in which surveillance schemes are to be deployed. They need a statement of the scheme's objectives. They need to know sufficient about the design features that they can apply reasonable tests to the scheme's feasibility, and assess its effectiveness under varying circumstances. They need the opportunity to apply systemic reasoning, in order to evaluate whether the design features can give rise to the claimed benefits.

(4) Justification for Proposed Measures

No measure should not be implemented unless its negative impacts are demonstrated to be outweighed by its benefits. It seems extraordinary that a case has to be mounted in support of such a straightforward contention. Yet national security and law enforcement agencies (NS&LEAs) have been permitted to make untested assertions about both threats to public safety and the benefits of surveillance measures in addressing those threats. The sacred cow of blind trust in NS&LEAs has to be put to death. Those organisations must be required to present their arguments, and defend them in public.

(5) Consultation and Participation

A further critical aspect of an open society is the ability of the public to participate in the debate. This enables testing of the information and arguments. But it also brings the many perspectives of a complex society to bear on the information and the declared objectives.

(6) Evaluation

Another form of normal service that needs to be resumed is the application of established techniques to the available information, in order to provide a basis for comparison among financial costs and benefits, on the one hand, qualitative factors on the second, and risks (and especially remote ones) on the third.

The technique of Privacy Impact Assessment (PIA) has been making headway during the last few years, and has attracted support now from such inherently conservative institutions as the Senate, the Privacy Commissioner, and in September 2007 the Australian Law Reform Commission (ALRC). An even broader notion of social impact assessment is crucial to the survival of an open society.

(7) Design Principles

One of the key features of the vignettes was the existence of positive instances of surveillance, both for individuals and society. Surveillance is not itself evil.

The problem has been the presumptiveness of its proponents, the lack of rational evaluation, and the exaggerations and excesses that have been permitted.

Proponents of surveillance have Design Principles that guide the creation of their systems. An alternative or complementary set of Design Principles is required, which guides the conception of schemes that do not threaten free society from within. Key examples includes the following:

- **Balance.** This must be achieved among the many competing values and interests, rather than a small cluster of ‘security’ imperatives dominating, and being protected by a veil of secrecy
- **Independent Controls.** These are essential in order to ensure that ‘national security’ interests are not the means whereby ‘national security’ assertions are validated
- **Nymity and Multiple Identity.** These must be recognised as natural human needs, and as keys to the freedoms in free society, despite the inevitability that they, like all freedoms, will be abused as well as used

Nymity encompasses both anonymity and pseudonymity, and is addressed in depth in Clarke (1999a). Genuine anonymity precludes the link being discovered between an identity and the entity or entities using it. It carries with it the risk of non-accountability. With pseudonymity, the link can be made, but its effectiveness depends on legal, organisational and technical protections, to ensure that the link is not made unless pre-conditions are fulfilled.

(8) Rollback

Restoring sanity to the processes whereby schemes are evaluated and designed is crucial, but far from sufficient. The depredations of the last 5 years are so great that rollback of the great majority of anti-freedom provisions enacted by Parliaments is necessary. The valuable Parliamentary Library catalogue of the actions of the federal parliament is frightening for its sheer length, even without consideration of its depth.

This is not to suggest that every provision of every amendment act must be overturned. National security and law enforcement agencies were, as they claimed, confronted by a variety of barriers that were accidental and inappropriate and needed to be overcome. On the other hand, inadequately brisk processes for the issue of warrants are not properly solved by creating extra-judicial warrants, but rather by a faster, online judiciary. And although telephonic interception warrants based on old, fixed-line numbering are inappropriate in the modern era of mobile phones, the balanced solution is person-based interception warrants, not the removal of controls.

7 Conclusions

A neologism can be a mere linguistic device intended to bring some intellectual

richness to a discussion. The English word ‘surveillance’ derives from the French ‘surveiller’, or ‘watch over’, which in turn derives from the French sur- and the Latin *vigilare*. So ‘überveillance’ takes a somewhat ambiguous Romance stem and imposes on it an abrupt and authoritarian Germanic prefix.

There are multiple flavours of ‘überveillance’, none of them comforting to someone who lives in the real Australian world of moderate daily dangers from cancer, heart conditions and road traffic, and of minuscule dangers from terrorism.

Unfortunately, as this paper has shown, all of the interpretations of ‘überveillance’ are descriptive of another reality, and one that has become rapidly more pervasive in the few years since the turn of the present century. We are confronted by the twin extremisms of religious fundamentalists in Muslim garb, on the one hand, and men in short haircuts chanting the mantra ‘national security’, on the other.

We need to ensure that the national security fundamentalists, who have ruled our lives for the last 5 years, are treated with the same seriousness as the terrorist threat within Australia, and are encouraged to return to the professionalism of the 1980s and 1990s, and respect for the free society that Australians believe they live in. This country wants neither ‘unter-veillance’ nor ‘überveillance’. It wants balance.

Original sources re überveillance

- Masters A. & Michael K. (2007) ‘Lend me your arms: the use and implications of humancentric RFID’ *Electronic Commerce Research and Applications* 6, 1 (March 2007) 29-39
- Michael K., Johnston K. & Michael M.G. (2007) ‘Consumer awareness in australia on the prospect of humancentric rfid implants for personalized applications’ Invited Industry Presentation, at the IEEE International Conference on Mobile Business, at <http://merc.mcmaster.ca/mBusiness2007/>
- Michael K., McNamee A. & Michael M.G. (2006) ‘The emerging ethics of humancentric GPS tracking and monitoring’ *Proc. Int’l Conf. on Mobile Business*, 25th-27th July 2006, Copenhagen, Denmark, 34-44
- Michael K., McNamee A., Michael M.G. & Tootell H. (2006) ‘Location-based intelligence – modelling behaviour in humans using GPS’ *Proc. Int’l Symposium on Technology and Society*, 8th-11th June 2006, New York City, 1-8
- Michael K. & Masters A. (2006) ‘Realised applications of positioning technologies in defense intelligence’ in H. Abbass & D. Essam (eds) ‘Applications of Information Systems to Homeland Security and Defense’ IDG Press, ch. 7, 167-195
- Michael K. & Michael M.G. (2005) ‘Microchipping people: the rise of the electrophorus’ *Quadrant XLIX*, 3 (March 2005) 22-33
- Michael, K., Michael, M.G. (eds), (2006a), ‘The Social Implications of Information Security Measures on Citizens and Business’, Wollongong:

University of Wollongong

- Michael K. & Michael M.G. (2006b) 'Towards chipification: the multifunctional body art of the net generation' Proc. Conf. Cultural Attitudes Towards Technology and Communication, 28th June – 1st July 2006, Tartu, Estonia, 622-641
- Michael M.G. (1998) 'The Number of the Beast, 666 (Revelation 13:16-18). An historical and theological investigation of Saint John's conundrum' Unpublished MA Honours Thesis, Macquarie University, NSW, Australia
- Michael M.G. (2000a) 'For it is the number of a man' Bulletin of Biblical Studies 19 (January-June 2000) 79-89
- Michael M.G. (2000b) '666 or 616 (Rev 13:18): Arguments for the authentic reading of the Seer's conundrum' Bulletin of Biblical Studies 19 (July-December 2000) 77-83
- Michael M.G. (2003) 'The Canonical Adventure of the Apocalypse of John in the Early Church (A.D. 96 – A.D. 377)' Unpublished PhD Thesis, Australian Catholic University, 2003
- Michael M.G. (2006) 'Consequences of innovation' Unpublished Lecture Notes No. 13 for IACT405/905 – Information Technology and Innovation, School of Information Technology and Computer Science, University of Wollongong, Australia, 2006
- Michael M.G. & Michael K. (2006) 'National security: the social implications of the politics of transparency' Prometheus 24, 4 (December 2006) 359-363
- Michael M.G. & Michael K. (2007) 'Überveillance: 24/7 x 365 People Tracking and Monitoring' Proc. 29th International Conference of Data Protection and Privacy Commissioner, at http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html
- Michael K. & Michael M.G. (2008) 'Innovative automatic identification and location-based services: from bar codes to chip implants' IGI Press, Forthcoming, 350
- Perusco L. & Michael K. (2006) 'Control, trust, privacy and security: evaluating location-based services' IEEE Technology & Society Magazine 26, 1 (Spring 2007) 4-16
- Perusco, L. & Michael, K. (2005) 'Humancentric applications of precise location-based services', IEEE Conference on e-Business Engineering, (18-22nd October 2005: Beijing, China), IEEE Computer Society, Washington, 409-418
- Perusco L., Michael K. & Michael M.G. (2006) 'Location-based services and the privacy-security dichotomy' Proc. 3rd Int'l Conf. on Mobile Computing and Ubiquitous Networking, 11-13th October 2006, London, England, 91-98

The author's papers on surveillance

This segment provides access to this author's previous papers on surveillance, indexed on his web-site.

- Clarke R. (1988) 'Information Technology and Dataveillance' *Commun. ACM* 31,5 (May 1988) 498-512, and re-published in C. Dunlop and R. Kling (Eds.), 'Controversies in Computing', Academic Press, 1991
- Clarke R. (1994a) 'The Digital Persona and its Application to Data Surveillance' *The Information Society* 10,2 (June 1994)
- Clarke R. (1994b) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' *Information Technology & People* 7,4 (December 1994) 6-37
- Clarke R. (1995a) 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism' *Information Infrastructure & Policy* 4,1 (March 1995) 29-65
- Clarke R. (1995b) 'A Normative Regulatory Framework for Computer Matching' *Journal of Computer & Information Law* XIII,4 (Summer 1995) 585-633
- Clarke R. (1997) 'Chip-Based ID: Promise and Peril' Invited Address to a Workshop on 'Identity cards, with or without microprocessors: Efficiency versus confidentiality', at the International Conference on Privacy, Montreal, 23-26 September 1997
- Clarke R. (1999a) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' *Proc. User Identification & Privacy Protection Conf.*, Stockholm, 14-15 June 1999
- Clarke R. (1999b) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' *Proc. 21st International Conference on Privacy and Personal Data Protection*, pp.131-150, Hong Kong, September 1999. Revised version in *Information Technology & People* 14, 2 (Summer 2001) 206-231
- Clarke R. (2001) 'While You Were Sleeping ... Surveillance Technologies Arrived' *Australian Quarterly* 73, 1 (January-February 2001)
- Clarke R. (2005a) 'Have We Learnt To Love Big Brother?' *Issues* 72 (June 2005)
- Clarke R. (2003) 'Why Biometrics Must Be Banned' Presentation at the Cyberspace Law & Policy Centre Conference on 'State Surveillance after September 11', Sydney, 8 September, Xamax Consultancy Pty Ltd, 2003
- Clarke R. (2005b) 'Human-Artefact Hybridisation and the Digital Persona' Background Information for an Invited Presentation to the *Ars Electronica 2005 Symposium on Hybrid - Living in Paradox*, Linz, Austria, 2-3 September 2005
- Clarke R. (2007) 'Business Cases for Privacy-Enhancing Technologies' Chapter

- in Subramanian R. (Ed.) 'Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions' IDEA Group, 2007
- Clarke R. & Stevens K. (1997) 'Evaluation Or Justification? The Application Of Cost/Benefit Analysis To Computer Matching Schemes' Proc. Euro. Conf. Infor. Syst. (ECIS'97), Cork, Ireland, 19-21 June 1997
- Wigan M. & Clarke R. (2006) 'Social Impacts of Transport Surveillance' Proc. RNSA Workshop on Social Implications of Information Security Measures upon Citizens and Business, Uni. of Wollongong, 29 May 2006, in Michael K. & Michael M.G. (Eds.) 'The Social Implications of Information Security Measures on Citizens and Business' Research Network Secure Australia, 2006, Chapter 2, pp. 27-44. Revised version published as Wigan M. & Clarke R. 'Social Impacts of Transport Surveillance' Prometheus 24, 4 (December 2006) 389-403

4

Appendix to what ‘überveillance’ is and what to do about it: Surveillance vignettes

Roger Clarke

Xamax Consultancy Pty Ltd

Visiting Professor at UNSW, ANU and the University of Hong Kong

Abstract

This document contains brief outlines of a range of diverse surveillance schemes. They are drawn from a wide variety of sources and experience.

Baby-monitoring

In response to sudden infant death syndrome (SIDS), and to enable parents and health carers to spend time away from the side of the cot, several technologies have been developed or applied. One is the fairly crude mechanism of periodically or continuously transmitting sound or pictures of the baby to a speaker or screen close to the carer. Potentially more effective forms of surveillance include devices that detect delay in breathing or heartbeat, or movement, particularly of the abdomen.

Acute health care

Automated monitoring is performed in many acute health care environments, including ambulances, emergency wards and Intensive Care Units (ICU). The monitoring focusses on the patient's key physiological characteristics, such as the cardio-vascular system and respiratory function.

Alerts are programmed to draw staff attention to parameters that have moved outside pre-set limits. The limits are set variously by the machine manufacturer, the hospital administration, and the particular nurse for the particular patient. There are different intensities in the alert signals, so that the more urgent ones can stand out. Individual devices generate different sounds depending on the level of the alert and the make of the machine.

Examples of alerts for which different sounds may be generated include:

- heart monitors, where the heart-beat is too fast, too slow, or absent – but often because the monitoring device has fallen off
- the intravenous (IV) machine has run out of fluid, the tube is kinked, it has an air bubble, or the battery has run down
- the blood-pressure cuff delivers a measurement that is too high or too low, or delivers an inconclusive result – or has fallen off
- the air mattress has a kink in the line, or has run out of battery
- the blood-oxygen-deprivation monitor registers too high, too low, no battery, a poor signal – or no patient

There are so many sounds, which are unique to each environment depending on machine makes and models, that even experienced nurses cannot recognise them all.

The devices keep bleating for attention, and they are attended to when the nurse needs them, or has a moment to address them. Any non-specialist visitors in the vicinity (or, much worse, concerned relatives visiting their loved ones) find the cacophony of alerts disturbing, and the apparent lack of attention to them even more so. The noise often drives the health clinicians mad, but most are also very useful.

Some of the serious alerts (such as those for respiratory and cardiac arrest) have been reproduced for other purposes (for example as ring tones on mobile phones),

and startle off-duty nurses when they are heard outside the health care context.

Staff movement monitoring

Some employers issue staff with tokens, emblazoned with the staff-member's name, photograph and perhaps other information. Such tokens commonly include machine-readable storage (magnetic stripes, chips, or contactless / proximity chips), which may contain the same data as is on the face of the card, but may also contain additional data-items. Some employers impose tokens that are woven into the uniforms that they provide to staff.

Staff may be under instructions to wear or carry their token, and they may be required to present it at various control-points on the employer's premises or campuses. Alternatively, the monitoring may be active throughout an entire controlled area, rather than only at control-points.

Carriage and presentation may be enforced by denying movement between zones (e.g. because a door cannot be unlocked or a boom will not open) unless the (or a) person presents (or is at least wearing or carrying) their own (or someone else's) token.

In addition to access control, some of these schemes provide current-location information to a controller. This can be used for both service delivery (e.g. directing an incoming phone-call to the nearest extension) and control applications. Schemes that log transactions also support movement tracking, retrospective analysis of movements, and potentially even real-time predictive capabilities relating to the person's likely destination.

Vehicle monitoring

A variety of organisations conduct surveillance of a variety of different kinds of vehicles. For example, employers, road service organisations, third-party fleet management companies, insurers, regulatory authorities, or law enforcement agencies may monitor load-carrying vehicles, taxis and hire-cars, but also private vehicles.

Vehicle movements may be logged by having them automatically report when they pass control-points (e.g. the entrances and exits of industrial or port complexes and loading/unloading bays, but also convenient networks of locations such as traffic lights). Alternatively, an on-board GPS device can compute the vehicle's location, enabling it to report its own position.

Data transfer can be done by active means (e.g. a transmitter on board initiating a communication to some other device), or passive means (e.g. a transmitter on a collecting device initiating a response from the monitored vehicle). In addition, on-board devices may monitor and report the performance of the vehicle, its engine and/or its load.

Among the characteristics that are measured may be apparent average speed over a distance or a period of time, and aspects of driver performance, particular time spent at, and not at, the wheel. (Excessive time at the wheel of a load-carrying

vehicle is a criminal offence, and excessive time not at the wheel may be against the interests of the vehicle's owner).

'Speed cameras'

A speed detection device can trigger a camera to capture images of the numberplates of passing vehicles. The registration-code can be extracted using pattern-matching recognition in a manner similar to Optical Character Recognition (OCR) for documents. A closely-related application uses a timing-based trigger to capture photographs of cars that run red lights.

Such installations may be in a fixed place for an extended period of time; or they can be mobile; and they may be declared or covert. The use of covert cameras for detecting speeding infringements has been shown to be more effective than declared cameras in securing generally lower traffic speeds. However, the use of covert cameras, especially in what are apparently safe areas and locations, has the effect of creating public cynicism about the motivation for, and the reasonableness of, the surveillance.

Use of the photos, and of the data inferred from them (in particular vehicle registration data, location and time), may be limited to a specific traffic law enforcement purpose, or function creep may occur.

Automated number plate recognition (ANPR)

The technology used for speed cameras can be applied much more broadly, as Automated Number Plate Recognition (ANPR). The data arising from ANPR can be used to automatically generate charges for road-usage, and can be linked with vehicle-registration databases to despatch notices of non-payment violations.

ANPR can also be used to compare passing registration-numbers against a 'blacklist'. This could reflect, for example, cars that have been reported as being stolen (and whose numbers have not yet been deleted from the database), or cars that are subject to an alert because they are recorded as having been used in the past by a person who is the subject of personal surveillance. A 'hit' on the blacklist may be used merely to generate a record for future data-mining, or to trigger action by law enforcement agencies, e.g. to intercept the vehicle on the basis of the suspicion generated by the entry in the database.

An early form of ANPR has been used in N.S.W. for many years, to monitor the time spent on the road and the average speed of heavy goods vehicles, and, in combination with drivers' log-books, driver work-hours. It has also been surreptitiously applied to cars, without apparent legal authority and without public disclosure, let alone debate.

ANPR is coming into general use in the U.K. for private cars. Its application has been mooted by at least two State Governments in Australia, but without any sign of an impact assessment being conducted at all, let alone independently from the police force.

Denial of anonymity on toll-roads

Use of public thoroughfares has always been essentially anonymous. Even on toll-roads, cash payment was available. Electronic payment was then added as an option. There are several ways in which anonymous electronic payment can be delivered, but most applications are either directly identified, or effectively identified because they involve credit-cards or debit-cards.

In recent years, some toll-roads have been permitted to rely on electronic payment mechanisms alone, and to remove all cash payment booths without providing an effective anonymous alternative. Melbourne CityLink appears to have been the first major thoroughfare in the world to deny anonymous travel. Sydney's M7 has been permitted to adopt the same approach. Neither company's web-site even addresses the question of anonymous payment.

The Privacy Commissioner has failed in her responsibilities under the Privacy Act s. 27 (1)(a)–(e) to ensure that breaches of the law, in this case of NPP 8, are avoided in the first place, or at least acted upon once they have occurred.

CCTV on railway stations, and everywhere else

There are occasional instances of violence on railways stations. Railway authorities have installed successive rounds of more equipment, and nominally more sophisticated equipment. Much the same has happened in shopping malls, cinema precincts and city streets more generally.

There appear to be very few occasions on which a criminal is apprehended as a result of the surveillance, or in which images from CCTV are instrumental in 'solving' a crime or achieving a conviction. People intent on committing a crime take steps to avoid being recognised, and even where the perpetrator takes no such steps the quality of images that is practicably achievable is limited. The primary functions of CCTV in relation to crimes that have already occurred appear to be to provide media interest, and to convey the impression that law enforcement agencies are 'on the job'.

Some deterrent effects do appear to exist, but only in respect of the space that is known to be subject to surveillance. The undesired behaviour appears to be largely displaced to unmonitored locations. In addition, 'crimes of passion' are largely unaffected. Even the claims of deterrence within the monitored area are in many cases unjustified: "[o]ut of the 13 systems evaluated, 6 showed a relatively substantial reduction in crime in the target area compared with the control area, but only 2 showed a statistically significant reduction relative to the control, and in 1 of these cases the change could be explained by the presence of confounding variables" (Gill & Spriggs 2005).¹ So in a study commissioned by one of the primary proponents, only 1 of 13 showed a statistically significant reduction.

1 Gill M. & Spriggs A. (2005) 'Assessing the impact of CCTV' Home Office Research Study 292, Home Office Research, Development and Statistics Directorate, U.K., February 2005

Goods monitoring

RFID tags can be used in supply chains from the manufacturer, via the transporter and wholesaler, to the retail outlet. This can provide benefits in stock control, for example where the goods are highly valuable, or where recalls may arise.

The RFID-tags may be left on the goods beyond the cash-register, in order to achieve a link between a category of product, or even a specific instance of a product, and the purchaser. This can be done openly or surreptitiously. And it can be done consensually, or pseudo-consent can be gained through coercion, or it can be imposed by the supplier, or it can be mandated by law.

The data arising from this form of surveillance can be used for a variety of purposes, such as after-sales service, consumer profile construction, consumer marketing, consumer tracking, and in the case of goods carried by the consumer (such as clothing) consumer association with a brand or style.

Goods monitoring is also applicable to dangerous materials, such as fissile material, explosives, materials that can be used to manufacture explosives, highly flammable materials (such as avgas), and to goods controlled for other reasons, such as pharmaceuticals particularly opium and coca derivatives. It is challenging to monitor bulk materials by means of RFID tags; but they are readily applied to storage facilities and containers.

Freight interchange-point monitoring

Locations in which goods are loaded, unloaded, and switched from one mode to another, may be subject to surveillance. This is particularly the case with loads that are intrinsically dangerous, or of high-value.

Such monitoring can assist in managing risks such as theft (of the load), pilferage (of some of the load), the introduction of additional materials into a load, tampering with the load, sabotage of the load, and insertion of an unauthorised load.

In association with this form of monitoring, the staff who are involved may be subject to various forms of indignity, including video-surveillance and recording while on the job, searches on completion of a shift, and 'positive vetting' by a government agency or private investigator as a condition of employment.

Financial transaction tracking

In the late 1980s, the Australian Government copied a US initiative and created what is now known as Austrac, to gather financial transaction data from financial institutions. The scheme was supposed to be a weapon against the drugs trade. Its justification has drifted with the fashions of the times, via money-laundering by organised crime, to the financing of terrorism.

There is very little evidence that it has ever delivered any benefits. But, rather than curtailing its activities, the Government and Parliament have submitted to the blandishments of law enforcement agencies, and have successively extended the

scheme's scope.

The most recent iterations have been simply scandalous, and completely beyond the boundaries of what a free society should be permitting. Under the 2006 'Anti-Money-Laundering and Counter-Terrorism Financing' Act (AML-CTF), financial institutions are now required to actively intrude into their customers' privacy in order to comply with 'Know Your Customer' (KYC) provisions, for reasons unrelated to banking; and to be actively suspicious about their customers, for reasons unrelated to the business relationship.

Yet worse, amendments introduced in 2007 propose to extend this to a range of small businesses, including real estate agents, financial planners, and jewellers. Business enterprises, large, and now small, are being forcibly enlisted into the business of spying on their customers. This is a pattern associated until now only with repressive regimes such as East Germany under the Stasi, and the People's Republic of China. It is extraordinary that Parliament could permit such a breakdown of the boundaries between the public and private sectors, and grant such extraordinary power to the national security and law enforcement apparatus.

Consolidation of agencies and databases

Meanwhile the mainstream mandarins have mounted a sustained campaign over more than 20 years, in an endeavour to develop a centralised scheme for the storage of personal data.

The centrepiece of the Australia Card proposal was a new database that the Health Insurance Commission wanted to be the hub of the centralised databank. When that was rebuffed, senior executives of the then Department of Social Security grasped their opportunity. They leveraged off DSS's substantial database and processing capabilities to morph it into Centrelink – a central government agency through which all of the c. 100 benefits paid by a score of agencies are funnelled. The organisation thereby became the hub database for the 25–35% of the Australian population who are recipients of some kind of benefit.

The next step in the process was the formation of a mega-ministry, currently called Human Services. Its purpose was to link Centrelink with the old Health Insurance Commission (now re-badged as Medicare). This, if it is allowed to be successful, would pool the resources of the two. Medicare covers virtually 100% of the population, because it is (or its core business is) the nationalised insurer.

Meanwhile, the 'Medicare' tag is being used in an attempt to broaden the agency's scope from health insurance to health data administration. The HealthConnect scheme adopted a centrist philosophy, but failed. The current NEHTA scheme is also being drifted from its initial federation and 'inter-operability' approach back towards the simplistic centrism that seems to be all that the mandarins are capable of understanding.

A further leg of the centralist agenda is the play by the Australian Bureau of Statistics (ABS) to become the national databank consolidator. In 2006, ABS

corrupted the Census by keeping in an identified form data relating to 1 million Australians. The ABS intends firstly linking all future returns into that pool of data, and secondly drawing data from the administrative collections of government agencies. The breach of trust with the Australian public will render the census inoperable within a few years. But this is of no consequence to the mandarins, because by then the agency's philosophy will have been switched from a trustworthy collector of original and unidentified data to a backroom consolidator of data from other databases.

The limited privacy law that was created in the late 1980s has already been undermined to the extent that the emergent consolidated databases are available to any agency that wants them. In any case, national security and law enforcement agencies are above the law in multiple senses, being exempt from privacy laws, being not subject to sanctions when they breach such limited constraints as do exist, and having been granted in recent legislation specific immunity for particular breaches.

National identification schemes

The tracking of financial transactions and the consolidation of personal data from multiple sources is only effective if individuals are constrained to a single general-purpose identity.

The first serious attempt at this was Australia Card Mark I (1985–87). It failed, because a very large proportion of the public emphatically opposed it once it became clear what it was.

In the ensuing years, the pre-existing Tax File Number (TFN) was expanded in scope. Successive Ministers and Prime Ministers breached their undertakings, and the scope was extended well beyond the boundaries that had been agreed at the end of the Australia Card debacle.

In the years following that, the Centrelink Access Number (CAN) was developed as an identifier that enables the inter-linking of data from multiple agencies involved in benefits payments.

Several attempts have been made to coordinate the driver's licence numbers issued by the States and Territories into a reliable national scheme, but this usually founders on inter-jurisdictional jealousies.

The natural next step is the 'Access Card', better understood as Australia Card Mark II. This is at heart a hub-database and a general-purpose identifier. (The card is, as always, a minor part of the overall scheme). The foundation element of the scheme would be registration interviews in which each individual would be effectively challenged to claim an existing identity recognised in government databases. To meet that challenge, every individual would have to respond to demands for documents, would be restricted to the use of just one identity approved by the government (possibly even a name that is dictated by the government), and would be required to use that single identity across all agencies. Services would become

dependent on the acquisition, carriage and presentation of the card.

The Australian public, once it appreciates what the 'Access Card' actually is, will reject it as emphatically as they did its predecessor.

Monitoring of human-attached chips

The miniaturisation of computers and storage has long since reached the point that small but quite powerful chips can be fitted into various carriers. The plastic-card-with-chip (often referred to as a 'smart card') has made very slow progress since its invention in 1974 and its initial deployments in the late 1980s. But suppliers are currently trying again, and this time they are attracting a little more interest from the major players: financial institutions and government agencies.

In addition to plastic cards, other carriers are possible. The chips used in 'contactless cards' are also used in 'RFID tags', which are appropriate for goods, and have been woven into clothing. A closely-related technology referred to as Near Field Communication (NFC) is being built into mobile phones.

This kind of chip has an antenna in which current can be induced by movement through a magnetic field, enabling transmission of a small amount of data, including the chip's unique identifier. Often the identifier of the chip, when combined with the location of the device that picked up the signal, is all that needs to be collected.

Various categories of livestock in the EU and the USA have been subject to imposed identification requirements from the early 1990s onwards. In Australia, a National Livestock Identification System (NLIS) exists. Breeding stock in particular have been commonly identified using tail-tags or ear-tags.

Humans have been subjected to the same technology as animals. The same kinds of chips have been installed in anklets and wristlets. These have potential application for people suffering senile dementia, and perhaps patients during pre-operative, operative and post-operative phases of their treatment. They have been imposed on several other categories of institutionalised people, in particular prisoners, and prisoners on parole. In the US, it appears that it is even being used for people who are on remand, as a substitute for bail or a supplement to it.

The actual use of the chips is varied. For a person in a relatively open senile dementia ward, for example, they could be used to raise alerts if the person approaches a perimeter, or has been immobile for a long period in an unusual location (e.g. neither their bed nor a sitting-room).

For prisoners, parolees and (in the US) people on remand, the intensity of the surveillance can range from occasional automated 'reporting in', via obligatory intentional reporting in by placing the device close to a fixed reader, to detection at the perimeter of areas of permitted movement.

Reports have suggested that, in the USA, in excess of 100,000 parolees and the remandees are wearing them, so the volume of data generated is vast. From the viewpoint of the person forced to submit to them, the intrusions can vary from mild to excruciating. A recent report on a 'celebrity' remandee (Lisa Nowak, a sometime

NASA pilot), showed how utterly degrading the process can be.

Monitoring of human-embedded chips

The kinds of chips in contactless chip-cards, RFID tags, and wristlets and anklets, have also been implanted directly into animals. A primary application has been for pet dogs and cats, to enable the return of lost animals to their owners. The conventional location for implantation has been the neck. One such service goes under the disarming brandname of Life Chip. In the livestock arena, moves are under way to migrate the chips from external tags to embedded ones.

Consensual implantation of chips in humans appears to have begun with a self-publicist academic who used it to open doors (in Reading UK). That was followed by fashion-driven implantation for access to a night-club (in Madrid).

Staff in a few companies (in the USA) and a government agency (in Mexico) have been inveigled into agreeing to the implantation of 'contactless chips' into their bodies.

Non-consensual applications have been touted in institutions of various kinds. In addition to prisoners, an often-mentioned category is senile dementia patients. It has been promoted as a means of patient management in hospitals.

The monitoring patterns would appear to be comparable to those for Human-Attached Chips, with the primary differences being the 'convenience' and non-visibility, the permanency, and the difficulty of removing it or suppressing its behaviour. These work variously to advantage (in some circumstances to some extent of the implantee, but mainly of the person doing the monitoring) and to disadvantage (almost entirely of the implantee, particularly in terms of the increased servility it entails).

Continuous monitoring of chips

The above discussions of human-attached and human-embedded chips assumed the monitoring activities to be sporadic or periodic, episodic and in any case occurring only within a limited span of time. It need not be so.

The ACT Government has stated its intention that the Territory's new prison, currently under construction, will use RFID tags to track prisoners. The scheme appears to involve permanent monitoring of all inmates, throughout the complex, every 2 seconds. It further appears that data is to be logged. It is therefore a means firstly of remote, automated power over prisoners, and secondly of enabling retrospective analysis and investigation.

Such effectively continuous and permanent surveillance is far less human even than the (often seriously unpleasant) relationships between prisoners and warders. It represents comprehensive denial of freedom, and comprehensive ceding of power to the surveillance organisation.

Permanent surveillance of prisoners was rejected in the late eighteenth century, in part because it was regarded as inhumane. At that time, the means was visual, in

the form of Bentham's 'panopticon'. The current proposal represents an even more insidious form of observation, because it is unseen, unrelenting and not equilibrated by any human element.

Such blanket electronic surveillance is unprecedented in Australia. This is a form of human degradation, rather than part of a plan to prepare prisoners for a positive return to life in the community. It would undermine the rehabilitation of offenders – even though the facility has been designed to house many who are due to be released back into the community in the near future. That in turns threatens public safety.

Further, the imposition of such a gross surveillance mechanism would set a precedent for the treatment of some people like cattle, pet dogs or pallets full of goods for sale, in, of all jurisdictions, the first in Australia to implement a Human Rights instrument.

Biometrics and foreigners

Biometrics, or measurements of some aspect of the human person or their behaviour, brings with it a vast array of intrusions into civil rights and privacy.

The Australian Parliament has legislated to impose biometric requirements on refugees, on applicants for visas, and on people infringing national boundaries (mainly fishermen). These powers have been subject to little or no consultative processes.

Aliens have almost no protections under Australian law, and refugees in particular are in a desperate state, and will concur with anything that a potential host-nation demands of them.

Biometrics and Australians

The collection of biometrics is an invasion of the physical person, acquiring something that is 'of' them, and in many cases imposing on a person's movements in such ways as demanding placement of the hand, thumb or eye in a zone dictated by an authority.

Biometrics schemes are technically very challenging, because it is very difficult to capture measurements reliably. Some biometrics may embody personal data, at least in the case of DNA. Biometrics create serious security problems, because the characteristics that are measured are not something that can be kept a secret. They can be captured surreptitiously and in some cases without the person being present (e.g. latent fingerprints, and body tissue and fluids).

A person's physical characteristics are unchangeable. This leads to seriously problematical risks such as 'entity fraud' (masquerade by someone using an artefact designed to replicate a person's biometric), the planting of evidence, and even the prospect of outright 'entity theft'. Recent concerns about 'identity fraud' and 'identity theft' pale to very little in comparison with such prospects.

Despite these enormous concerns, a number of applications of biometrics have emerged, including workplace bundying-on/off, building access control, electronic

access control (for logging on and off computer systems), device (PC and phone) locking/unlocking, and prison-visitors.

In the area of DNA, voluntary provision lasted a mere decade. The State has begun giving itself enormous powers to gather DNA, initially from long-term prisoners, then from prisoners, and most recently from arrestees. Protections that had been developed over many decades in relation to fingerprints have been ignored. The slippery slope from freedom to State control has been measured in a few short years.

International travel

Before the early 1920s, documents such as letter from a patron were useful in crossing national borders, but not necessary. The international passport system was established in a climate of mass movements of displaced persons following World War II. It became increasingly common for governments to demand documents that evidenced a person's nationality. Passports have since been converted into a near-universal requirement for international travel.

Government agencies sustained the 'managed hysteria' opportunity presented by the post-September 2001 terrorism threat in order to arrange parliamentary approval for a raft of changes to the Australian passport scheme. These swept away decades of case law, reduced the rights of citizens in relation to passports, and established a new form of passport that embodies various technologies.

The new document includes a contactless chip, which contains at least the same personal data as the printing on the document and the previous magnetic-stripe, but in a form that is machine-readable provided that the reader has access to a cryptographic key. There remain doubts about its security.

The legislation granted freedom to the Passports Office to implement biometrics, in whatever manner it sees fit, subject only to convincing their own Minister of the day. This was done in such a manner as to avoid even mentioning the word or concept of biometrics. This represents an extraordinary delegation of power to public servants.

At this stage, the agency has implemented only a low-integrity scheme based on so-called 'facial recognition' technology. The very probable failure of the scheme will be available as an excuse to implement successive biometric schemes, progressively creating a government-controlled pool of biometrics of Australians, available for sharing with friendly governments and other 'strategic partners'.

The biometric passport, coupled with the reduced rights, represent a leap in the power of the State over individuals. The passport has been transformed into a general identity document, with apparently enhanced credibility through the inclusion of a biometric element. This creates the risks of wider permeation of biometric identifiers, and of function creep towards use of passports in circumstances other than at national borders. The ability of the agency to achieve the wide and uncontrolled powers that it has, without so much as the pretence of public consultation, augurs very ill for the survival of freedom of anonymous movement

within the country's borders.

Domestic travel

In general, identification has not been required in order to travel within free countries in the past. Other than during World War II, public areas have almost never been blocked to public access, although exceptions have arisen, such as the occasional visits of security-hypersensitive US Presidents, that result in 'lock down' of segments of major cities and of major arteries in order to give free passage to privileged 'motor-cades'.

In the air travel industry, the practice grew up during the second half of the 20th century of requiring that tickets carry the identity of the person they were purchased for. The reason for this had nothing to do with security. It was an endeavour to avoid the emergence of a secondary market in tickets, and hence ensure that all of the revenue that could be extracted from air travellers went to the airline.

In recent decades, national security and law enforcement agencies have leveraged off the identification carried on air-tickets for commercial reasons, and sought to impose a requirement for air-travellers to identify themselves. The US in particular has created specific barriers not only against anonymous domestic air-travel, but also against travel by individuals who appear to use the same name as a person of interest (the so-called 'no fly' lists). This has led to quite ridiculous false positives, including Yusuf Islam (once known as Cat Stevens), and US Senator Ted Kennedy. The 'no fly' list has had many failures, yet very little success.

Anonymous travel has always been a feature of road travel, but this has been seriously compromised by toll-roads that demand identified forms of payment. The first was Melbourne CityLink, but three segments in Sydney have also recently become identified-payment-only roads. The problem is compounded by the 'public-private partnership' nature of these 'public infrastructure' operations. This seriously compromises data protections, because each has access to data properly available only to the other, and the schemes impose criminal sanctions in respect of civil matters.

There has also been plenty of scope for anonymity with public transport ticketing, compromised only in such cases as long-term season tickets, typically for a year, and in some cases for heavily-discounted tickets, particularly for people with disabilities. Schemes that are currently being trialled (mostly unsuccessfully) in N.S.W. and Victoria appear to deny a practicable anonymous option, and perhaps any anonymous option at all.

These together conspire to create a context in which individuals can be tracked and located through domestic transport infrastructure. In short, constraints are being enabled that were hitherto only implemented in seriously un-free countries like apartheid-era South Africa and the Soviet Union.

It is reasonable to expect that 'control orders', having survived the test of constitutionality, may be a testing-ground for extra-judicial constraints on travel.

Service denial

Many kinds of services involve positive discrimination, in that they are only available to particular individuals, or individuals who satisfy particular eligibility criteria. Typical of these are seniors' discounts and disabled parking.

One form that has already been implemented on occasions is entrance monitoring. For example, some individuals may be denied access to sporting or entertainment venues, particularly fans / patrons who have previously exhibited undesirable behaviour at that or a similar venue. It has been claimed that casinos use so-called 'facial recognition' technology to detect problem gamblers banned from the premises (including both those who are problems for themselves or their families because they are compulsive, and those who are problems for the casino because they are effective).

Mechanisms already exist whereby a great many services could be denied to specific individuals. International travel is tightly regulated, and various categories of people are denied access to it (e.g. the stateless, and those whose country refuses to issue with a passport or 'exit visa', or whose passport has been withdrawn or surrendered). In the USA, domestic air travel is denied to many people who either refuse to provide evidence of identity or whose names are the same as names on the 'no-fly' list. The increasing preclusion of anonymous travel on Australian roads and public transport systems creates a vast array of possibilities for service denial. So do the tight identification requirements in the financial services sector.

An Australian Government initiative in 2007 changed welfare distribution mechanisms for aboriginals in the Northern Territory to limit the use of a substantial proportion of the payments to specific categories of consumer items. It would have been unreasonable to expect that the scope of negative discrimination and service denial would be restricted to aboriginals. Any form of welfare payment may become subject to diktat of such kinds. A Parliamentary Committee Recommendation emerged within weeks of the N.T. legislation passing, proposing similar measures for benefits-recipients with drug habits.

Many other possibilities exist. For example, security clearances, which in a few short years have exploded from a narrow category of occupations to a vast array of paid and even unpaid positions, can readily be used as the means for denying access to locations and services.

Identity denial

A further step available to a powerful State is to deny a person legitimate existence. The notion was pioneered by John Brunner's 'The Shockwave Rider' in 1975, and popularised in a film in the 1990s, 'The Net'. It has physical parallels in refugees without documentation stranded in airports, and in the Pacific Island 'solution' for 'boat people'.

5

Owning identity- one or many- do we have a choice?

Marcus Wigan

Oxford Systematics

Professorial Fellow, University of Melbourne

Abstract

Identity is the key to linking records and multiple identities are the key to maintaining social functioning with appropriate anonymity, while retaining accountability. This paper addresses these factors and adds the issue of ownership of one's own 'identity'. Collapsing what are currently entirely legal multiple identities into a single identity through direct or indirect digital means has implications for dataveillance and surveillance. The lack of transparency in most such emergent developments amplifies an increasing asymmetry in information between government and major organisations - and citizens, the subject of this effect.

Keywords: identity, ownership, surveillance

1 Introduction

The rapid growth of databases, biometrics and RFID and other identity related technologies are approaching a critical mass as a potential means of controlling the population. The critical aspects of these diverse technical advances are the links between identity and existing and accelerating intensification of dataveillance capacities. Taking one example: DNA databases are perhaps the most salient, but their comprehensive application is still to materialise in terms of a critical contribution on a large scale. The legal infrastructure to expand them more rapidly is already within the capacities enabled by recent legislation, but the cost and complication (and indeed vulnerabilities) in building such databases mean that at present we can consider them as simply fresh opportunities for function creep. Saliency, DNA might have, but its high profile potential is dwarfed by the already present risks inherent in the many other cross-linkages now being enabled directly. These links may be direct (via formal data matching legislation) or indirect by rapidly expanded powers ranging from authority to secretly monitor parties on a prospective (trawling) basis creating assemblies of data from many sources. The linkages enabled by a “unique identity” are central to both direct and indirect means of data and physical surveillance. Identity is now commonly publicly discussed and treated in legislation as if it were a unique item. This supposition has many ramifications and impacts. One might surmise that these were emergent – or intended: in either case the social impact is not widely appreciated.

2 What is identity?

This is a basic question, and is assumed to be obvious. The classic *Compact Oxford English Dictionary* (OED) (1984, p. 1368) definition is, after discussing sameness, likeness and oneness:

1. The quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration: absolute or essential sameness; oneness
2. The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality.

This definition demonstrates the ambiguity of the word. A clear distinction is drawn in the dictionary between the various definitions and usages of the term ‘identity’ and the quite separate term ‘absolute identity’. Once again we profit from examining the full version of this definitive work on language and find that the confusions and asymmetric interpretations used for the word are just as varied as the views on what identity comprises. The penetrating point made by the OED authors is the choice of the phrase “in all circumstances.” This is the critical factor that makes the verification of identity in one context assumed to apply to all contexts. This is now the central issue.

There are few situations where complete and definitive verification of identity is possible, and the tendentious term “Identity Card”; simply makes the implied assumption that the token (the card) is indeed the person. This is actually a big step, and one that has in the past considerably harder to do ‘in all circumstances’ than it may seem.

“Identification” as a verb is the task that such tokens are aimed at addressing. Again, identification for what? It is hard to find a case where the context does not define the level of accuracy and reliability of the process of ‘identification’. Passports are specifically intended and agreed upon as the relevant token for border crossing (and in fact nothing else). Yet the idea of a passport as a high grade token for assertion or verification of identity is almost irresistible as a simple means of establishing the identity of a person in situations far removed from any border. The intrinsic value of a passport as an identity token is explicitly exploited by hotels everywhere as a means of securing payment from the client and to satisfy police and surveillance records. Function creep will always be with us.

The most common form of identity is one’s name, but as there may be many with the same name the addition of a photograph provides additional discrimination. Yet an original birth certificate showing only the name is also deemed to be a high quality form of identity verification. There are clearly far more factors involved in a ‘simple verification of identity’ than meets the eye, and the OED has long been onto it.

In this paper we address the different factors that comprise identity in two ways:

1. The ability to achieve an accepted ‘identity’ as oneself by the use of tokens or other forms of associated factors
2. The level to which a restriction to a single token-certified ‘identity’ can or should be used for all purposes.

Once these rather different common interpretations of ‘identity’ are appreciated, there then becomes a clear need for multiple ‘identities’ sufficient for any specific purpose (usually a transaction, access or an event) requiring an assumed reliable association between a person and a token. Many situations require only a temporary identity: a movie ticket is a simple anonymous example usually with a linkage period requiring a simple identity association of a very short duration (ie the holder is identified as authorized to enter the cinema: a very clearly defined context)– and with no attributes to be linked to a specific person required: the holder gets entry, non holders do not. Transaction completed. Others require stronger links to the person and for longer. But it is clear that not only is there a working acceptance of an ‘adequate’ verification of identity, but there is also recognition that not all events or transactions require the same identity to be used.

A professional woman may continuously operate in her unmarried name, a stage name, a *nom-de-plume* – or her husband’s surname in different circumstances. There is no suggestion made that this is in any way a criminal or even dishonest

behaviour. On the contrary, many authors, actors, police, psychologists, witnesses etc all have valid and compelling reasons to be able to live under different identities. In the case of family violence or witness protection the lack of any linkages is imperative, sometimes for sheer survival. How is has it been possible to have multiple identities in this way? Simply because if people undertake their legal responsibilities with various bodies and the community this is a basic freedom – but this freedom depends on trust and genuine security and credible security at that.

The Tax Office has long had taxpayers paying tax on activities illegal at the time (prostitution being one example), and generated a solid reputation for keeping the ‘tax payer’ identity separate and unlinked to other forms of identity. The current environment has dismantled these protections against linkage between legal multiple identities both by data matching and by huge reductions in the constraints on a range of public officers in many areas of state activity to access and link multiple identities. This not only reduces the trust in these bodies, but also makes many people vulnerable in new ways. Family violence victims and witness protection programs are now not the only ones at risk. The pressures to eradicate multiple identities are associated mainly with efforts to link different forms of real time and recorded data and associate it with each individual for efficiency in establishing identity, and over time to build a cumulative and increasingly cross-linked picture of the person or thing (‘entity’) concerned. Tracing of behaviour, movements and characteristics and location of animals serves a similar purpose in scientific studies. Treating people as animals to be traced continuously wherever they go and whatever they do is an interesting perspective which is a disturbing facet of *überveillance* (Michael & Michael, 2006), and emphasizes the potentially dehumanizing aspects of asymmetric information secured and held by anonymous third parties.

3 The basis of identity verification

The efforts to make a token identical to a person are now mediated by computers and communications where a single tag or number enables a person to be the subject to both intentional and generally undirected data trawling and integration. The results of such trawls come up with links between people and activities but are vulnerable to data quality, and other processes which may have been done for quite different purposes. The issue of an initial verification of identity (say for a national ID card) is one of data quality, and this is an expensive commodity. The processes outlined for both the UK and the Australian national identity cards under consideration have huge holes in them. These include the limited basis for verification before a person is approved as having demonstrated their own identity, and the very limited time allowed in most planning for such systems for this task to be executed. In the Australian system it is proposed that a brief training of Post Office workers will suffice to execute this in a few minutes.

For some a completely documented life record is easily supplied, but for others even securing people who have known them by sight and joint activities will be

a real problem. Yet once the ID is issued it is assumed to be the unique identifier linked to the person in some real way. This will inevitably corrupt the ID database from the very start. This means that false positives will be widespread not only for the person involved but other parties who have met 'higher' standards of verification. This is an easily accepted argument but is very misleading. Personal knowledge of a person covers many different attributes than simple appearance, yet a passport or driver licence with a photo ID on it is regarded as 'more reliable'. This is in spite of a large volume of evidence that people are very poor at matching photos to the relevant individual, as indeed are biometric facial recognition techniques at this point.

So how do we assess these issues? As the major reason for government pressures for ID uniqueness, matching tokens is essentially to facilitate management and control of the population by longitudinal and cross-sectional linkages. The rhetoric is to confirm right to access some location or service, or to be able to undertake a transaction but this introduces a fundamental asymmetry in the relationship: false negatives in token matching deny access to those with the rights to them, with absolutely no penalty to government at all while false positives allow such access and also contaminate the records of others thereby in both cases disadvantaging the population as a whole. This basic issue of a single 'do all' identity is simply not understood by many. This is not uncommon in cases of non-transparent information asymmetries between governments and the population as a whole. It is however an area where governance and identity interact. A complementary view on some of these issues is given by Clarke (1994) but the over riding social aspect of such mappings onto a single unique (and indeed easily copied) digital identity is that of the inevitable denials of service, and most likely to those most in need of them as these are the people who will tend to have most difficulty in establishing their own identity in the first place.

4 Other mechanisms

In non-governmental interactions trust is a major feature of transactions, and a recommendation, an introduction or even a simple referral can be quite sufficient for most transactions. However, trust does not figure highly in everyday transactions with governments or large organisations. This links governance to transparency in the mediation of such interchanges requiring identity. Efficiency and cost savings are major drivers in the long-standing bureaucratic thrust towards universal unique identification. The role of trust in government surveillance in the United States was discussed by Staples (1997) four years before the cultural shifts following the destruction of the World Trade Centre. He argues that:

The movement to a post modernist culture of corrections is one of normalising social control over all aspects of life – fit the power inequity aspects of privacy measured by others (p. 128).

A society in a culture of surveillance, a society of judges exercising the

power to punish everywhere, a society increasingly lacking in personal privacy and individual trust and a viable public life that supports and maintains democratic values and principles (p. 129).

Were it not for function creep and the opportunistic approach of enforcement and other dataveillance and surveillance bodies, there might have been a high integrity medical ID card in Australia by now: yet this is one of the declared objectives of the Australian governments ID card initiative which has been described as carrying out many further functions from the start: demonstrated function creep before the system is even properly designed. The trust factor is still largely there between the community and the medical professions. Medical administration roles in handling and linking such data is not usually seen as part of the patient-doctor relationship. There are also asymmetries of information holding between doctors themselves is a consequence of the ownership of patient records by the doctor that treats the patient. These may be seen as barriers to efficiency or as good faith in very private information held in trust – or, as is now increasingly the case in other fields, valuable commercial micromarketing data.

In summary, identification is clearly contextual, and efforts to move towards a unique token as formal ID can be seen to automatically trigger issues of governance, transparency and trust. This perspective appears to replicate many of the aspects of the original Australia Card, the current Australian and UK ID card debates, but moves it on from the purely political aspects of power assertion to the mechanisms we have discussed.

5 Implementing identity

So far we have avoided discussing the meaning of the tokens that are used as proxies or in support of identity establishment or verification. This now needs closer examination, as there may be many tokens associated with a single identity even when the individual is using one of several multiple identities. A digital identity is an assemblage of token ('identifiers') that describe that identity. One person may have many personas (or operating or perceived identities) but for any particular function or transaction requiring the establishment of an identity for a specific purpose or occasion, there are usually only a few identifiers used, and these may not be the same for transactions with another body or organisation.

In the contemporary, complex and high-paced world, organisations seek to manage identities on the basis of their digital identities. The quality of the management will reflect the quality of the digital identity. But that will vary enormously depending on the usual data quality characteristics (accuracy, precision, completeness, timelines, etc.), and especially on the quality of the acts of associating data with identities. This leads us to the concept of a digital identity, which comprises solely a set of data associated with a specific person or thing. This set of data is assumed to be an accurate representation of the person or thing (the generic term for this is 'entity', and is a physical item or person). There is a special set of digital

data that is associated directly with an entity. Examples are:

- in the case of a person, biometrics;
- in the case of a person or thing, embedded RFID chips etc.

In such cases the entity is its own identifier, and this is invariant on circumstances or situations requiring identity establishment or verification.

Organisations are seeking to manage entities on the basis of their digital entities. The quality of the management will reflect the quality of the digital entity. But that will vary enormously depending on the usual data quality characteristics, and especially on the quality of the facts of associating data with entities. If biometrics prove to be practicable in enough settings, the quality of digital entity may be higher than could ever be the case with digital identity. The impact and implications are far more drastic, however, because the level of social control that can be achieved will chill individual behaviour, social discourse, economic innovation, and political thought and speech.

This qualitative difference between intrinsic (entity bound) identifiers, which stay the same for all circumstances, leads to an automatic deletion of multiple digital identities, as such a unique key to a person is virtually irresistible to both commerce (know your customer and tailor services to their known wealth or other accumulated identifiers integrated over time), and to government for cumulative comprehensive population tracking and surveillance).

6 Links between surveillance and identity

There is little difference in principle between:

1. An anklet with a GPS tag that is fitted to a prisoner to constrain his or her location, and to allow real-time monitoring as well as historical tracking of all his or her activities, and;
2. An RFID location and access control badge that must be worn to work to access or move about a specific building or area;
3. An injected RFID chip to allow repeat Club patrons to be allowed to enter the premises– and of course potentially to be monitored by other detectors.

The real difference is the voluntary nature of some of these identifiers (injection of an RFID chip) and the nature of the usages made of the data stream that follows: voluntary or not (intrinsic identifiers such as biometrics or DNA are not voluntary).

Context is all. As long as the context is the domain solely, of say a Club premises, then multiple identities are still possible outside that domain – but if this unique tag (or biometric) is accessed by other organisations, then (in the case of biometrics) an indelible trail is cumulatively created: one that can be readily extended backwards and well as forwards, and over many organisation both prospectively or historically.

This process is the collection of a surveillance data set. The links between surveillance and identity depend critically on the tokens or identifiers used to establish identity. Persistent identifiers specific to the person or thing (entity) make

it very difficult to avoid function creep.

The scope of intrinsic identifiers is global, the differences are in the ease or otherwise of securing them. As costs drop in securing and converting intrinsic identifiers then the application widens rapidly. DNA databases used to be collected solely from criminals, but are now routinely collected from suspects who may be innocent. Function creep has already occurred with the general public in the area of an event now having their DNA required as prospective scanning and profiling tool with the data being retained to build on ever expanding databases. In whatever way it proceeds and under whatever guise, such libraries of intrinsic identifiers can only grow and expand.

National ID cards are specifically designed to make this possible. There is no need for automatic ticketing cards to include high grade identification, but the emergent practice is that it will be. The anonymous token (paper ticket) simply does not provide enough marketing and trace information for the various parties, commercial and enforcement, seeking it as a by-product of your purchase and use of a right to travel from A to B. The days of anonymous travel or movement are numbered.

As such cumulative records emerge, then the existence and use (let alone the well documented tendency for abuse) of surveillance data will affect the social space of all the surveillance subjects (ordinary citizens). Such constraints on social space have a disproportionate effect on individuals who need to live with multiple identities (or to have to alter) their identities.

The only way to conserve the existing legal right to operate using multiple identities is to require a privacy audit of all systems and digital tokens used. This is quite evidently not in the interest of many parties seeking such surveillance and retrace capacities, and, as a result is highly unlikely to occur. Abuse, as is so well documented already, (e.g. Independent Commission against Corruption, 1992) will occur- and both the social space will be reduced and the security of individuals concerned will become at greater risk as a result. The shrinking of social and physical space has already been observed. As a result of the intrusive and extensive biometric data capture and distribution at the borders, there are numbers of people who have simply stopped travelling on routes that require entry to the USA.

7 Collapsing identities

The surveillance aspects of digital identity tracking also lead to a substantial contraction of the social and transactional spaces that people can use. Examples are already plentiful. CentreLink requirements for identity documents from the very groups most likely to not ever have had them, simply are a plausible and defensible means of denial of access. Currently the tests required to establish identity include known persons and other normal social means of adequate identification for the purpose in hand but once unique (or quasi-unique) digital identity tokens are held by all, then there will be two major effects:

1. Such low grade data entering the system as many simply will not have the levels of documentary 'evidence' of their identity (leading to both positives and false negatives in the use of the supposedly unique digital identity), and a general reduction of the integrity of the whole system
2. Lack of the token will enable denial of service.

It is clearly necessary to introduce a concept of *Contextual Sufficiency* into identity establishment. This has been in the past implied in almost all transactions, but will be lost if all one's identities are required to be collapsed into one via the existence of a unique identifier; and if this is a biometric, the contextual variations and relaxations will be lost. Once the principle of contextual sufficiency is lost, then validation failures and multiple matches will have pervasive and widespread negative effects on individuals- and this will not be restricted to those with a major need for multiple identities right now.

The marked increase in information asymmetries between the observed and the observers will require compensating social action. One essential action must be the removal of politicians exemption from privacy laws applied to their data collections. Other less obvious steps will be needed as well to provide transparency and accountability for linked or potentially linkable information resources. Brin (1998) discusses an interesting highly speculative but stimulating case of full symmetry of information between the surveillers and the surveilled. If only such a scenarios could be realistically envisioned, let alone implemented, but it goes against the pervasive enforcement organizations and political structures in most present cultures and societies.

It is clear from public debate that the pervasive impact of collapsing identities to one for each person introduces many restrictive and disturbing side effects and vulnerabilities. These will grow with time, rather than diminish, due to the retrospective matches that will become possible.

8 Ownership of identity

As almost all tokens of identity are now handled in a digital form, operational identity is becoming a bundle of data items. Who owns these? The current TRIPS (trade-related aspects of intellectual property rights) protocols of the World Trade Organisation (WTO, 2007) is very clear on this:

1. Assemblages of public data have copyright in that collection, and:
2. Such assemblages may be created automatically by a computer and still retain a copyright.

So if an organisation or organisations make the effort to collect data about you that can be linked via intrinsic identifiers in a digital form, not only will they own the digital form of the identifiers but also the full set of tokens the comprise your digital identity. The Government asserts copyright over public information

and extracts a monopoly rent for it.¹ How profitable it will be to own peoples own digital identity. As this is clearly what is implied by the current database and copyright law. In a real sense you will then not own your own identity. A highly valuable commodity, as identity theft is now demonstrating. Only here it is not the transaction done in your name but the very data that comprises your own identity that is alienated from you. The potential for this outcome was discussed at the time of the TRIPS negotiations by Wigan (1992).

9 Conclusion

The growing use of digital identifiers takes on a very special set of social impacts if collapsed by the wide use of biometrics and especially with ID cards linked to biometrics, however unreliable. Once identity becomes the presentation of a digital dataset, then the very ownership of ones own 'identity' then comes into question. While this may not prove to be a problem, the collapsing of our daily multiple identities into one has far wider implications than are immediately obvious. This paper has simply introduced a few of the implications. The term *überveillance* is correctly applied to the combination of powers and asymmetries and consequences of these trends.

References

- Brin, D. (1998). *The Transparent Society*, Addison-Wesley, Reading Massachusetts.
- Clarke, R. (1994). *Human Identification in Information Systems: Management Challenges and Public Policy Issues* <<http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html>> (accessed 4 October 2007).
- Independent Commission against Corruption (1992). *Report on the Unauthorized Release of Government Information*, 3 vols., ICAC Sydney.
- Michael M.G. and Michael K. (2006). "National Security: The Social Implications of the Politics of Transparency", *Prometheus*, 24(4), pp. 359-363.
- Staples, W.G. (1997). "The Culture of Surveillance: Discipline and Social Control in the United States", in G. Ritzer (ed.) *Contemporary Social Issues Series*, St Martins Press, New York.
- Wigan, M. R. (1992). "Data ownership", in R. A. Clarke & J. Cameron (Ed). *Managing Information Technologies, Organisational Impact II*, 1 (pp. 159-169). Amsterdam, North-Holland.
- WTO. (2007). *Trade-Related Aspects of Intellectual Property Rights*, <http://www.wto.org/english/tratop_e/trips_e/trips_e.htm> (accessed 4 October 2007).

¹ This is a regular complaint in Australia about collections of data made and held by the Australian Bureau of Statistics, and in the UK about the holdings of mapping data by the Ordnance Survey – where they have attracted a widespread "give us back OUR data" movement.

6

Opposing surveillance

Brian Martin

Professor, School of Social Sciences, Media and Communication,
University of Wollongong

Abstract

If surveillance is potentially seen as unfair, then it is predictable that its proponents will use a number of methods to reduce public concern: cover up surveillance activities, devalue targets and opponents, offer plausible interpretations for actions, use official processes that give an appearance of fairness, and intimidate and bribe targets and opponents. Opponents of surveillance can be more effective by being prepared for these tactics and working out ways to counter them.

Keywords: surveillance, tactics, opposition, outrage, resistance

1 Introduction

Over the years, many people have opposed surveillance, seeing it as an invasion of privacy or a tool of social control. Dedicated campaigners and concerned citizens have opposed bugging of phones, identity cards, security cameras, database linking and many other types of surveillance. They have lobbied and campaigned against abuses and for legal or procedural restrictions. Others have developed ways of getting around surveillance.

In parallel with resistance, there have been many excellent critiques of surveillance, exposing its harmful impacts and its role in authoritarian control (e.g., Dandeker 1990; Gandy 1993; Garfinkel 2000; Holtzman 2006; Lyon 1994, 2003; Marx 1988; Murray 1993; Rosen 2000). However, comparatively little is written about tactics and strategy against surveillance. Indeed, social scientists have little to say about tactics and strategy in any field (Jasper 2006: xii–xiii). My aim here is to present a framework for understanding tactics used in struggles over surveillance.

Actions that are seen to be unfair or to violate social norms can generate outrage among observers (Moore 1978). Nonviolence researcher Gene Sharp (1973: 657–703) found that violent attacks on peaceful protesters — something that many people see as unjust — could be counterproductive for the attackers, generating greater support for the protesters among the protesters’ supporters, third parties and even the attacking group. Because of this potential for attacks to be counterproductive, attackers, by design or intuition, may take steps to reduce possible outrage. By examining a wide range of issues — censorship, unfair dismissal, violent attacks on peaceful protesters, torture and aggressive war — a predictable pattern in tactics can be discerned: perpetrators regularly use five sorts of methods to minimise adverse reactions to their actions (Martin 2007).

1. Cover-up: the action is hidden or disguised.
2. Devaluation: the target of the action is denigrated.
3. Reinterpretation: plausible explanations are given for the action.
4. Official channels: experts, formal investigations or courts are used to give an appearance of justice.
5. Intimidation and bribery: targets and their allies are threatened or attacked, or given incentives to cooperate.

This is called the backfire model: when these methods are insufficient to dampen public outrage, the action can backfire on the perpetrator. However, backfire is rare: in most cases, the methods work sufficiently well to minimise outrage.

Consider an example different from surveillance: police use force in arresting someone. This has the potential to cause public outrage if the force used is seen as unnecessary, excessive or vindictive. Police in these circumstances regularly use one or more of the five methods. If possible, they undertake the arrest out of the public eye. They refer to the person arrested as a criminal or by derogatory terms. If challenged, they claim arrestees were resisting and that using force was necessary

and carried out according to protocol. They refer those with grievances to official complaints procedures, which almost always rule in favour of the police. And they may threaten the arrestee with criminal charges should they make a complaint (Ogletree et al. 1995).

On 3 March 1991, Los Angeles police arrested a man named Rodney King, in the course of which King was hit by two 50,000-volt tasers and beaten with metal batons more than 50 times. This arrest would have gone unnoticed except that George Holliday, who lived nearby, recorded the beating on his new videocamera. When footage was shown on television, it caused a massive public and political reaction against the Los Angeles police. Holliday's videotape cut through the normal cover-up and allowed viewers to judge the events for themselves, overriding the police's interpretation of the events and the media's normal police-sympathetic framing (Lawrence 2000). Nevertheless, in the ensuing saga the police and their supporters used every one of the five methods of inhibiting outrage — though, unusually, in this case their efforts were unsuccessful in preventing a huge backlash against the police (Martin 2005).

Tactics for and against surveillance can be analysed using the same framework. The foundation for public outrage is a sense of unfairness. This is certainly present at least some of the time: people may see surveillance as an invasion of privacy (as with hidden video cameras), as a tool of repression (as in monitoring dissenters) or a tool of exploitation (as in monitoring of workers). The very word “surveillance” is a tool in opposing it, because the word has such negative connotations.

A sense of unfairness is not inherent in the act of observing someone or collecting and analysing data about them. People's sense of unfairness is the subject of a continual struggle, with privacy campaigners trying to increase concern and purveyors of surveillance techniques trying to reduce it. Methods to inhibit or amplify outrage are used within the prevailing set of attitudes and in turn affect those attitudes.

Given that some people see surveillance as inappropriate, unfair, dangerous or damaging, there is a potential for resistance and hence it is predictable that one or more of the five methods of inhibiting outrage will be deployed. In the remainder of this paper, I look at each of the five methods of inhibiting outrage and ways to challenge these methods.

The five-method classification used here is a convenient framework for examining tactics for and against surveillance. To use this framework does not require actors to be consciously engaging in a struggle, as many are simply reacting to the circumstances in which they find themselves. For those who are concerned about surveillance, though, it is useful to think in terms of tactics and strategies.

2 Cover-up and exposure

Surveillance is commonly carried out in secret. When people don't realise it's happening, they are far less likely to become concerned about it. The secrecy

covering surveillance is part of a wider pattern of government and corporate secrecy (Roberts 2006).

Political surveillance of individuals is normally done surreptitiously. Bugs are installed in residences; telephones are tapped; remote cameras record movement; police in plain clothes observe at a discrete distance. There is an obvious reason for this: targets, if they know about surveillance, are better able to avoid or resist it. But secrecy is maintained beyond operational necessities: in most cases, the existence of surveillance is kept secret long afterwards, often never to be revealed. Exposures may require exceptional circumstances (Marx 1984), such as the collapse of East Germany's communist regime or the "liberation" of FBI files at Media, Pennsylvania in 1971 by the Citizens' Commission to Investigate the FBI (Cowan et al. 1974). When surveillance is exposed, for example FBI surveillance of individuals such as Martin Luther King, Jr. and John Lennon, it can cause outrage. The revelation that the National Security Agency had been spying on US citizens since 2002 caused a massive adverse reaction.

Employers sometimes do not want to tell workers they are being monitored, when there is a possibility this may stimulate individual or collective resistance. (On other occasions employers are open about monitoring, when this serves to induce compliance.)

Under the US Patriot Act, the FBI can obtain secret warrants to obtain records from libraries, Internet service providers and other organisations. The organisations subject to this intrusion cannot reveal it, under severe penalties. This draconian enforcement of secrecy serves to reduce personal and popular concern about surveillance, for example when the Patriot Act is used against non-terrorist groups such as antiwar protesters.

In some cases, surveillance becomes routinised, so cover-up is less important. In many areas, camera monitoring is carried out openly: it is possible to observe oneself, on a screen, walking into a shop. On the other hand, some forms of surveillance are hidden so effectively that they are completely outside of most people's awareness, for example collection of web data, meshing of database files, police checks on car licence numbers and recording of bank transactions.

The importance of low visibility in enabling surveillance to continue and expand is apparent through a thought experiment: imagine that you received, at the end of every month, a list of instances in which data had been collected about you, by whom and for what purpose. Imagine knowing whether you had been placed on a list to be denied a loan or a job.

Exposing surveillance is crucial to challenging it. Exposure requires collection of information, putting it into a coherent, persuasive form, providing credible backing for the evidence, and communicating to a receptive audience. Sometimes a single person can do all of these steps, collecting information directly and publishing it on the web. Normally, though, a chain of participants is involved, for example an insider who leaks documents, a researcher who prepares an analysis, a journalist

who writes a story and an editor or producer who publishes it. Campaigners help in exposure, as with Privacy International's Big Brother Awards for organisations with bad records in threatening privacy.

3 Devaluation and validation

If a person is perceived as unworthy, then people don't get as upset when bad things are done to them. Executing an innocent person is seen as outrageous; executing a serial murderer elicits less concern. The inmates of the US prison at Guantánamo were portrayed as the "worst of the worst"; abrogating the civil rights of people painted as terrorists was accepted by much of the population, at least initially.

It is to be expected, therefore, that proponents of surveillance will denigrate targets as a means to justify their operations. Three popular labels for targets of surveillance are criminals, terrorists and paedophiles. Who could be opposed to fingerprinting welfare recipients if it prevents cheating? Who could be opposed to monitoring of emails or cameras on every street corner if it helps deter paedophiles? Furthermore, devaluation is extended to those who oppose surveillance, who are said to be defending criminals, terrorists and paedophiles.

The trite expression "If you have nothing to hide, you have nothing to fear" is built on an implicit devaluation: if you're concerned about privacy and surveillance, you must have something to hide, which implies you're guilty and devious (Marx 2007). Therefore, surveillance seems to be justified.

One way to challenge devaluation is to emphasise the essential humanity of every individual. A powerful way to do this is to make targets human, by using names, photos and personal details. Australian David Hicks was incarcerated without trial at Guantánamo for over five years without trial, and stigmatised by the Australian government as a terrorist. Opponents of Hicks' treatment were eventually able to generate concern, using photos of Hicks to make him appear as an ordinary person. Hicks' father Terry spoke out on his behalf, as did his US military lawyer Michael Mori: having valued allies helps counter devaluation.

The same principle applies to validating targets of surveillance. Personal stories of individuals subject to political surveillance are potent tools for validation. For example, Penn Kimball (1984) in his book *The File* poignantly tells of discovering spy agency files about himself in 1978, three decades after they were initiated on a flimsy pretext. The 2006 German film *The Lives of Others* encouraged the viewer to identify with the targets of East German political surveillance and with the Stasi agent who came to sympathise with them. Personal stories of innocent victims of surveillance gone wrong are similarly powerful. A few people will respond to abstract arguments about human rights; many more will respond to personal stories. George Orwell's novel *1984*, a powerful portrait of a dystopian future, uses the personal story of Winston Smith to make larger political points.

4 Interpretation struggles

Proponents of measures that increase surveillance typically provide a justification, often in terms that resonate with widely accepted values. Identification of vehicles is to monitor traffic, detect lawbreakers or collect congestion fees; compilation of corporate databases is to increase efficiency and provide better customer service; cameras are to prevent crime; identity cards are to reduce fraud; baggage checks are to prevent terrorism. The most effective justifications have an element of truth, sometimes quite a large element. The increase in surveillance is simply a by-product, deemed insignificant and unproblematical.

Proponents typically exaggerate the effectiveness of measures. One powerful way to do this is to treat effectiveness as self-evident. Cameras on public streets deter crime, of course. Who could doubt it? Seldom is empirical evidence provided; perhaps little is collected or sought. This is an especially potent technique because it doesn't require the public to trust what authorities say, because members of the public are the ones drawing the conclusion. Airline travellers who, in order to fly, tolerate pointless checks through bags and removal of fingernail files and nail clippers may not question the assumption that such measures are deterring terrorists.

Proponents seldom discuss alternative ways of accomplishing the same goal. An alternative approach to aircraft hijackings is to train passengers in how to communicate with each other and organise to overcome terrorists, as occurred spontaneously on 9/11 United Airlines flight 93 (Scarry 2003). This approach involves trusting passengers and increasing their awareness and skills rather than treating them as potential terrorists. It is seldom mentioned by government authorities, who focus exclusively on measures that give agencies greater power. Radical alternatives are seldom articulated. Rather than keep extensive records on poor people to prevent them cheating on welfare, an alternative is to increase the level of free distribution. For example, free or low-cost food could be provided to anyone who wants it, an expansion of current welfare services. This would reduce the need to monitor individuals.

Problems with surveillance systems are typically said to be rare or non-existent. Sometimes, though, surveillance abuses are publicised, for example cases in which someone has been denied a loan due to incorrect information on a database. These are explained away as rare mistakes. Then there are the systemic abuses, such as the illegal selling of information from databases — for example those held by police — to private investigators and others. These are commonly attributed to rogue operators. The system of information collection is not blamed.

In summary, proponents of surveillance typically provide a plausible justification for measures, exaggerate or simply assume their effectiveness, ignore alternatives and explain away abuses as rare events due to rogue elements.

Opponents of surveillance have challenged every one of these interpretative techniques. Most importantly, they have highlighted the potential of existing

or potential systems to increase unnecessary and damaging surveillance. They have challenged claims or assumptions about effectiveness. They have proposed alternatives. And they have argued that abuses are symptoms of flawed systems.

One of the key elements of interpretation struggles is the language used. Proponents of intrusive measures almost never use the word “surveillance.” For example, cameras are called security cameras, not surveillance cameras. What about opponents? It is common to refer to use the language of “privacy,” which resonates with people’s concerns about the sanctity of private life. But privacy rhetoric has disadvantages, in particular that it is personal in focus, whereas surveillance is largely an institutional practice (Stalder 2002).

John Gilliom (1994) analysed the arguments used for and against compulsory drug testing in US workplaces in the 1980s. Proponents justified testing mainly in terms of safety at work, the drug problem generally and the productivity of drug users, whereas opponents mainly cited privacy followed by legal rights, testing error and other concerns, of which surveillance was mentioned by only a few. Gilliom argues that rights discourse was limited because the law is constructed to serve the powerful, and improvements in drug test methods addressed concerns about errors while allowing the testing to continue. The implication of Gilliom’s analysis is that opponents’ choices of arguments against testing can have a major influence on the success of opposition generally, because arguments lead to particular ways of challenging testing — including legal methods, a form of official channel.

5 Official channels

Courts, ombudsmen, grievance procedures and formal inquiries are examples of official channels. Many people believe that these provide justice. They do in quite a few cases, but when the perpetrator is far more powerful than the victim, official channels typically give only an illusion of justice. For example, some people who speak out in the public interest are nominally protected by whistleblower laws, but in practice these laws provide little or no protection (De Maria 1999). Official channels are typically slow, focused on procedural technicalities, dependent on experts (such as lawyers) and keep matters out of the public eye. They are the exact opposite of using publicity to mobilise public concern. Regulatory agencies for protecting privacy fit this mould.

Some opponents of drug testing in US workplaces took cases to courts, some of which opposed testing. However, the Supreme Court supported testing, so the legal approach failed overall (Gilliom 1994). Along the way, it soaked up a large amount of money and effort, took a long time, distracted energy away from other opposition options, and enabled proponents to achieve an authoritative legal opinion in favour of testing.

In Australia, the Privacy Commissioner, a government-funded office, can receive complaints and make judgements. But its role is severely constrained. The Commissioner has to operate within the current law, which for example does not

cover private sector uses of information. As soon as the law is changed, for example to allow another type of database matching, the Commissioner must accept this as the new framework for judging privacy concerns. Furthermore, the Commissioner cannot do much to oppose any practices that it judges to be violations. Anyone who looks to the Privacy Commissioner for relief from actual invasions of privacy, or to halt a new practice, is likely to be disappointed (Davies, 1996).

In most countries, government agencies charged with protecting privacy have been ceding ground for decades. There are some legislative and administrative constraints on surveillance, to be sure, but agencies provide little for anyone seeking redress. If you know or suspect that your employer has been monitoring your email, that your telephone company has been releasing logs about your calls or that information about your purchases is on a corporate database, you can approach any number of agencies, most likely to find out that either the practice is legal, that you have no right to know, or that no information is available to you.

There are many people working in or with agencies who are dedicated to the public interest. The problem is not motivation but the role of agencies in the social structure: they are given limited mandates and inadequate funding, must operate according to bureaucratic regulations and have little or no capacity to initiate significant change. They can be simply overwhelmed by contrary forces, such as the post-9/11 war on terror. Finally, a really effective agency, that gets in the way of powerful interests, is likely to have its funding cut or mandate restricted.

The implication is that opponents of surveillance should not look to official channels as the solution. Stronger laws and well-funded oversight bodies can be worthwhile, but it is a mistake to put too much energy into promoting them, especially because reforms can so easily be rolled back (Olmsted 1996). Increasing public concern should be the primary goal, and that means publicising the issues, gaining supporters, building alliances and developing campaigns. If these efforts are effective, it is likely that governments will create or bolster official bodies to try to convince people that the problem is well in hand.

In 2005, the British government introduced the Serious Organised Crime and Police Act, which includes a provision requiring protesters within one kilometre of Parliament Square to obtain a permit, a requirement that allows files on radicals to be compiled. To even wear a T-shirt with a slogan requires a permit. Activist comedian Mark Thomas (2007) promoted “Mass Lone Demos” by thousands of people with diverse causes, for example some opposing the Iraq war and others whimsically opposing the month of February, overloading the police with permit requests and making fun of the law.

6 Intimidation, bribery and resistance

Surveillance measures can be intimidating: no one likes to imagine that their conversations and actions are being recorded. Having one’s photo and fingerprints taken by a government body can be humiliating and stigmatising. Intimidation

serves to reduce expressions of resistance. Local critics of surveillance abuses are likely to come under increased surveillance themselves, rather like the way peace activists can end up on US government no-fly lists. (Prominent critics may be a bit safer, because surveillance of them, if discovered and disclosed, could generate more publicity).

There is also a parallel process of encouragement to go along with intrusive measures. If you supply your identification card, you have access to government services. If you allow cookies, you have access to certain websites. If you allow your licence number to be recorded, you can drive on certain roads. Surveillance often comes along with benefits. Accepting the benefits creates a psychological debt: a greater willingness to accept surveillance.

To oppose surveillance, there need to be some people willing to resist. Insiders, with knowledge of abuses, can leak information to public critics. Investigative journalists can probe political surveillance. Citizens can expose what has happened to them. This is resistance aimed at mobilising wider awareness of surveillance and its damaging effects.

Many individuals attempt to avoid or disrupt surveillance, for example by giving incorrect information on forms, joining campaigns against identity cards, or damaging speed cameras. If actions are widely taken up, they can have a major impact and can stimulate development of new methods of resistance. Using and promoting encryption is an example. If everyone puts some encrypted files on their computer and sends occasional encrypted emails, even if they have nothing to hide, this makes it harder for snoops to determine who is worth watching. This is especially important in repressive regimes, where use of encryption might be seen as implying subversive activities. Struggles to enable access to encryption technology are a vital part of resistance (Schneier & Banisar 1997).

Gary Marx (2003) has distinguished 11 different types of individual resistance to surveillance, for example avoiding detection, blocking intrusive measures, refusing to provide information, and encouraging surveillance agents not to enforce regulations. He gives examples of each type of resistance and argues that there will be an ongoing struggle between controllers and resisters, with total control being unrealisable.

Methods of intimidation are often linked to cover-up. Beginning in the 1970s, *CovertAction Information Bulletin* challenged secret agencies by exposing the identities of undercover CIA agents; in response, the US Congress in 1982 passed a law against this. This law later led to a giant scandal when government officials revealed the identity of CIA agent Valerie Plame in reprisal against her husband Joseph Wilson for questioning false claims used to justify the 2003 invasion of Iraq (Wilson 2005).

This case suggests that data-gathering can sometimes be turned against powerful groups. Normally, the groups that instigate and run surveillance systems, such as politicians, employers, top bureaucrats and spy agencies, are not equally subject to the techniques they use against others. For example, employers may monitor workers but workers are seldom able to monitor employers to the same extent. Collecting

data about the rich and powerful, putting them on a par with others, challenges and deters intimidation. In other words, if the rich and powerful want surveillance, then make sure the searchlight is turned on them as well as others.

7 Conclusion

In order to gain insight into struggles over surveillance, it is useful to analyse the methods typically used by perpetrators of perceived injustice to reduce outrage over their actions. The promoters of surveillance commonly hide their operations, denigrate the targets and critics of surveillance, give plausible justifications for operations, set up oversight bodies that have little power to challenge anything more than minor violations of regulations, intimidate opponents and provide incentives for cooperation. To refer to “promoters of surveillance” and describe their methods does not imply any conscious intent on their part: many of them do not see themselves as promoting surveillance, but rather as cracking down on crime, providing better consumer service or increasing the efficiency of service systems: they believe in their own interpretations of what is happening. Likewise, to speak about the methods used to reduce outrage need not imply any conscious strategy: these methods are simply intuitive or obvious ways to reduce opposition.

The value of looking at methods used by promoters of surveillance is that it gives guidance for opponents. Some of these are fairly obvious, including exposing abuses and explaining what is wrong with surveillance. Others are less so, in particular being sceptical of official channels and instead mobilising support. Over the decades, many critics of surveillance have advocated stronger regulations, yet these have been regularly superseded by new technologies, overturned by emergency powers, undermined by loopholes and made hollow by weak enforcement. According to the model used here — reflecting studies of a wide range of domains — relying on regulations is seriously flawed: to a considerable extent, it gives only the appearance of dealing with problems, dampening public concern while allowing developments to continue.

To challenge surveillance, according to the framework used here, public outrage needs to be fostered in a range of ways. The model gives guidance for actions that are likely to be effective, but it does not say who will or should take action. Dedicated opponents have too often been overwhelmed by the forces promoting surveillance. In such circumstances, even the best tactics may be inadequate.

Nevertheless, it is far too soon to lose heart. Many other social movements — against slavery, for women’s emancipation, against environmental destruction — only gained widespread support after decades or centuries of exploitation and damage. Surveillance may become more ubiquitous and insidious, but there remains a strong reservoir of public concern about privacy, autonomy and freedom. Today’s critics and campaigners are laying the basis for a future challenge to emerge. Understanding tactics can help make that challenge more effective.

Acknowledgements

I thank Gary Marx, Steve Wright and two anonymous referees for valuable comments on a draft.

References

- Cowan, P, Egleson, N, Hentoff, N with Herbert, B & Wall, R 1974, *State secrets: police surveillance in America*, Holt, Rinehart and Winston, New York.
- Dandeker, C 1990, *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day*, Polity Press, London.
- Davies, S 1996, *Monitor: extinguishing privacy on the information superhighway*, Pan Macmillan, Sydney.
- Davies, SG 1997, 'Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity' in *Technology and privacy: the new landscape*, ed PE Agre & M Rotenberg, MIT Press, Cambridge, MA.
- De Maria, W 1999, *Deadly disclosures: whistleblowing and the ethical meltdown of Australia*, Wakefield Press, Adelaide.
- Gandy, OH 1993, *The panoptic sort: a political economy of personal information*, Westview, Boulder, CO.
- Garfinkel, S 2000, *Database nation: the death of privacy in the 21st century*, O'Reilly & Associates, Sebastopol, CA.
- Holtzman, DH 2006, *Privacy lost: how technology is endangering your privacy*, Jossey-Bass, San Francisco.
- Jasper, JM 2006, *Getting your way: strategic dilemmas in the real world*, University of Chicago Press, Chicago, IL.
- Kimball, P 1984, *The file*, Allen & Unwin, London.
- Lawrence, RG 2000, *The politics of force: media and the construction of police brutality*, University of California Press, Berkeley, CA.
- Lyon, D 1994, *The electronic eye: the rise of surveillance society*, Polity Press, Cambridge.
- Lyon, D 2003, *Surveillance after September 11*, Polity Press, Cambridge.
- Martin, B 2005, 'The beating of Rodney King: the dynamics of backfire', *Critical Criminology*, vol. 13, no. 3, pp. 309-326.
- Martin, B 2007, *Justice ignited: the dynamics of backfire*, Rowman & Littlefield, Lanham, MD.
- Marx, GT 1984, 'Notes on the discovery, collection, and assessment of hidden and dirty data', in *Studies in the sociology of social problems*, ed JW Schneider & JI Kitsuse, Ablex, Norwood, NJ, 78-113.
- Marx, GT 1988, *Undercover: police surveillance in America*, University of California Press, Berkeley, CA.
- Marx, GT 2003, 'A tack in the shoe: neutralizing and resisting the new surveillance', *Journal of Social Issues*, vol. 59, no. 2, pp. 369-390.

- Marx, GT 2007, 'Rocky Bottoms: techno-fallacies of an age of information', *Journal of International Political Sociology*, vol. 1, no. 1, pp. 83-110.
- Moore, Jr., B 1978, *Injustice: the social bases of obedience and revolt*, Macmillan, London.
- Murray, G 1993, *Enemies of the state*, Simon & Schuster, London.
- Ogletree, CJ, Prosser, M, Smith, A & Talley, W 1995, *Beyond the Rodney King story: an investigation of police misconduct in minority communities*, Northeastern University Press, Boston.
- Olmsted, KS 1996, *Challenging the secret government: the post-Watergate investigations of the CIA and FBI*, University of North Carolina Press, Chapel Hill, NC.
- Roberts, A 2006, *Blacked out: government secrecy in the information age*, Cambridge University Press, New York.
- Rosen, J 2000, *The unwanted gaze: the destruction of privacy in America*, Random House, New York.
- Scarry, E 2003, 'Citizenship in emergency', in *The Best American Essays 2003*, ed A Fadiman, Houghton Mifflin, Boston, 223-242.
- Schneier, B & Banisar, D 1997, *The electronic privacy papers: documents on the battle for privacy in the age of surveillance*, Wiley, New York.
- Sharp, G 1973, *The politics of nonviolent action*, Porter Sargent, Boston, MA.
- Stalder, F 2002, 'Opinion. Privacy is not the antidote to surveillance', *Surveillance & Society*, vol. 1, no. 1, pp. 120-124.
- Thomas, M 2007, "'Tony Blair is a cult'", *New Statesman*, 25 April, viewed 24 September 2007, <<http://www.newstatesman.com/print/200704250005>>.
- Wilson, J 2005, *The politics of truth: inside the lies that put the White House on trial and betrayed my wife's CIA identity*, Carroll & Graf, New York.

Message in a bottle: Stored communications interception as practised in Australia

Rob Nicholls¹ and Michelle Rowland²

¹Consultant, ²Lawyer, Gilbert + Tobin

Abstract

This paper applies a commercial analysis to the operation of Australia's interception powers in practice, drawing on the experience of the authors in advising operators in this area. The Blunn Report, the recent passage of legislation which permits access to stored communications and the introduction of further amending legislation in 2007 are indicative of the dynamic and increasingly intrusive nature of lawful interception and access powers. This paper discusses the current framework for the interception of stored communications and argues that short message service messages and most instant message services are not caught by the current legislative drafting. The paper shows that despite this drafting deficiency, carriers are responding to stored communications warrants as if the services were capable of lawful interception. The paper goes on to critically assess the recently introduced Bill in terms of the implications for operators in this area and the extent to which the rationale for such change has been clearly espoused. We examine the interaction between the Attorney-General's Department and the relevant policy and regulatory actors in the telecommunications sector. We conclude that the Australian telecommunications legislative and regulatory regime, with its emphasis on industry self-regulation, is being subsumed by the objectives of the Attorney-General's Department and that operators in the sector are responding to the spirit, but not the letter, of the law which facilitates lawful interception and access.

Keywords: lawful interception, stored communication, SMS, instant message, reasonable assistance

1 Introduction

This paper takes a practical approach to the activities associated with lawful interception of both telecommunications and stored communications under the current legislative regime. Whereas lawful interception of voice communications has been practised for many years, there is an increasing demand from law enforcement agencies for access to other forms of communication. In 2006, this led to amending legislation which permitted appropriate agencies to gain access to stored communications with the intention of being able to access each of emails, short message service messages and instant messages. This paper discusses the implications that arise from the change in requirements for access to communications and the practical implementation of such access.

We begin by considering some of the literature on interception of communications 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 consider the current legislative framework and the drafting which must be interpreted by telecommunications carriers in Australia. After this, the paper describes some practical cases 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 case studies and draw conclusions.

2 Background

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 voice and access to stored communications was provided 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.

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 (**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 (Bellovin et al. 2006; Landau 2005). 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 (ETSI 2007; Fonknechten et al. 2004; Gidari 2006; Gratzner et al. 2006; Miettinen 1999; Milanovic et al. 2003a; Milanovic et al. 2003b; Open Mobile Alliance 2005; Street 2003).

Much of the focus of the debate over interception capability has been in respect of voice over Internet Protocol (**VoIP**) (Del Bianco 2006; Drinan et al. 2005; Miller et al. 2005). Whereas the amendment to CALEA to introduce an obligation for interception of VoIP services was a new obligation, this is not the case in Australia. The *Telecommunications Act* 1997, imposes an obligation on all carriage service providers with facilities in Australia to maintain an interception capability (s.324(2)) and to provide assistance to relevant agencies (s.313(3)). The amending legislation which created the current *Telecommunications (Interception and Access) Act* 1979 described below did not relax that obligation.

3 Interception and access

There are three broad interfaces between telecommunications operators and law enforcement agencies. These have been standardised (ETSI 2007) and are summarised in Table 1.

Essentially, the 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. 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 information as to communications 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. This type of information would include, in respect of an identified individual, the addresses or phone numbers of communications to and from that individual and 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.

Table 1 – Handover interfaces

Relationship between carriage service provider and law enforcement agencies	Deliverables	Handover Interface reference
Ongoing	Service and service level agreements (these agreements may derive from regulatory obligations or, in the case of Australia, be contracts between the carriage service provider and the law enforcement agencies.	HI1
Established for the duration of delivery of communications related information in response to a request for assistance	Information relating to the specified type of communications of a target individual including the nature of that communication, the parties to that communication, the location of the target and the commencement and cessation time and date of the communication	HI2
Established for the duration of delivery of communications in response to a warrant	The content of the communications	HI3

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 information about communications and the content of those communications.

As a practical matter, operators of large telecommunications networks acquire switches from vendors which incorporate lawful interception ports into their equipment. This means that the delivery of interception-related information or communications content is readily facilitated and can be simply provisioned using electronic control of the switching device. However, network elements such as email systems and short message service systems do not have the same inbuilt lawful interception access as voice telecommunications equipment.

4 The legislative framework

4.1 The core interception framework for calls

The primary objective of the *Telecommunications (Interception and Access) Act 1979* (the **Act**) is to protect the privacy of personal communications by generally

prohibiting interception of those communications, subject to limited exceptions in which privacy is outweighed by other considerations. As such, the Act provides a general prohibition on interception of communications passing over a telecommunications network unless the interception is in the national interest, or is in connection with inquiries related to certain offences (s.7(1) of the Act).

The Act operates concurrently with the primary telecommunications law, the *Telecommunications Act 1997*. Part 13 of the *Telecommunications Act* establishes a primary prohibition against disclosure of information or documents that relate to the supply of carriage services to a person, and the affairs or personal particulars of such persons. It is a catch-all prohibition which is replicated in nearly every telecommunications law in the world. Although not explicitly stated in the law, it recognises that the privacy of a communications is a fundamental right which must be protected in all but the most extreme or logically permissible circumstances. Failure to comply with the primary prohibition in Australia is an offence punishable on conviction by up to 2 years imprisonment.

Part 13 of the *Telecommunications Act* also sets out this limited range of exceptions to the primary prohibition against the disclosure of information. These include cases where the information is disclosed to assist ASIO, a regulator, or where the relevant person has given their knowledge or consent to the disclosure of their information. The important aspect to note about Part 13 is that it is a primary prohibition which only permits disclosure on a specified exceptions basis. It is not an authorising provision for any person to demand disclosure of information.

The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (the **2004 Amending Act**) introduced the concept of stored communications and provided that a stored communication could be intercepted without the need for a telecommunications interception warrant. Whilst it introduced the concept of stored communications, the 2004 Amending Act did create some confusion regarding the particular situations in which a stored communications is deemed to be passing over a telecommunications system. The *Telecommunications (Interception) Amendment Act 2006* (the **2006 Amending Act**) clarified the procedures around the interception of stored communications and implemented a separate warrant regime for accessing stored communications.

4.2 The 2006 Amending Act

The 2006 Amending Act contains a general prohibition on the interception of stored communications in the same manner as telecommunications interceptions are prohibited in s.108 of the Act. It also provides for certain exceptions in which a stored communication can be intercepted. These include where access is authorised by a stored communications warrant, where access is authorised by an interception warrant and certain other specific circumstances in s.108(2) of the Act.

Relevantly for our discussion, a “stored communication” is defined to mean a communication with the 4 specific elements prescribed in s.5 of the Act:

- the communication must have passed over a telecommunications system;
- the communication must not be passing over that or any other telecommunication system;
- the communication must be held on equipment operated by the telecommunication carrier at its premises; and
- the communication must be accessible to the intended recipient of the communication.

The concept of “passing over” is clarified within the 2006 Amending Act by providing that a communication that is passing over a telecommunications system continues to do so until it can be accessed by the “intended recipient” of the communication in s.5(f) of the Act. “Intended recipient” is defined as in s.5(g) of the Act as:

- individuals to whom the communication is addressed to;
- if not an individual, any person within a group who is able to access communications sent via that address; or
- any person, or any employee or agent of the person, who has control over the telecommunications services to which the communication was sent.

The Act also defines the concept of accessing a stored communication to mean listening to, recording or reading a stored communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient in s.6A(a). The distinction of knowledge means enforcement agencies are only regulated by the stored communications regime when they are acting covertly in accessing these communications. When acting overtly, existing access and compulsion powers of the enforcement agencies remain applicable.

4.3 The warrant regime

The 2006 Amending Act inserted a separate warrant regime for access to stored communications held by a telecommunications carrier. ASIO and enforcement agencies are treated differently within the regime.

ASIO can access stored communications in the same manner as it is able to intercept communications under a named person warrant in s.9(1a) of the Act. This means the Attorney-General may issue warrants to ASIO to intercept communications where the communications are being used by a person who is “reasonably suspected” of engaging in (or likely to engage in) activities prejudicial to security and the interception will, or is likely to, assist ASIO in its function of obtaining intelligence relevant to security.

In contrast, a stored communications warrant can be made available under a different and arguably lesser threshold, substantively set out in s.116 of the Act, to an enforcement agency that is investigating a “serious contravention”; or an offence which is punishable by a maximum period of imprisonment of at least three years, or a pecuniary penalty of at least 180 penalty units. Indeed this is not a trivial threshold, however the point to note is that the scope of offences defined as “serious

contraventions” prescribed in s.5E of the Act is finite, but the decision to issue the warrant remains discretionary and based on the information made available to the authority issuing the warrant. Additionally, all enforcement agencies (criminal, civil and public revenue agencies) can obtain access to a stored communications warrant, whereas only law enforcement agencies (the Australian Federal Police, the Australian Crime Commission and declared State and Territory law enforcement agencies) can obtain an interception warrant.

A stored communications warrant is only in force until it is first executed or 5 days after the day it is issued, whichever occurs first, pursuant to s.119(1) of the Act.

4.4 Application of the legislative framework to email communications

Just as the Act imposes a primary prohibition against interception, stored communications are also subject to a primary prohibition against access. It is an offence, subject to penalties of 2 years imprisonment and/or a significant monetary fine, for a person to access a stored communication or otherwise authorise access without the knowledge of the recipient or the sender of the communication in s.108 of the Act.

“**Access**” is defined to mean listening to, reading or recording a communication. The threshold, like the other tests in the Act, is whether or not the intended recipient had knowledge of the access in s.6AA.

Two initial observations are relevant:

- The Note to the prohibition against access in s.108 of the Act specifically excludes accessing communications that are no longer passing over a telecommunications system from the intended recipient. It appears this is intended to exclude the forwarding of communications, and the recipient of that forwarded communication accessing that message (either email, SMS or MMS).
- The knowledge threshold in the definition of “access” refers only to the knowledge of the intended recipient. However, the threshold in s.108 which states the prohibition against access refers to the knowledge of neither the intended recipient or the sender of the communication. One would think that the appropriate drafting would refer to a prohibition against access without the knowledge of either the sender or the recipient of a stored communication.

The conjunctive definition of a “stored communication” as noted above, appears well-suited to describing an email communication. An email indeed becomes stored when it ceases passing over a telecommunications system, is held on equipment operated by and in the possession of a carrier (for example, the carrier’s server or network equipment); and is unable to be accessed without the assistance of an employee of the carrier (excluding a person who is not a party to the communication, ie the sender or a recipient).

This describes the normal functionality of an email communication. It leaves the server of an end user, which may be a company, and is carried by an ISP hosted on a carrier's network. That ISP of course may be the ISP of the host carrier (for example, BigPond on the Telstra Network). The electronic message is then carried to the ISP of the recipient's ISP located on the host's carrier network, to the server of the end user as delivered to the recipient.

4.5 SMS/MMS communications

The definition of a stored communication, combined with the clarification of the "passing over" concept (noted above), becomes problematic for SMS/MMS communications. The Act has been constructed to describe the email scenario where a communication passes over a system and is then accessed by a recipient. The only other opportunity for access arise on the carrier side, by reference to the equipment that stores the email communication on the carrier's side.

In contrast, SMS/MMS communications are "store and forward" messages. Unlike the direct transmission of an email from server to server via a network, SMS/MMS messages are relayed by the sender's device indirectly to the recipient via a short message service centre or a (SMSC) or a mobile message service centre (MMSC). The SMS/MMS message sits in the SMSC/MMSC which is essentially a processor. The processor attempts to forward the message to the recipient device, often making several attempts over a defined period, such as 24 hours, before the delivery is successful. This is set out in Figure 1. It is informative to note that the when a mobile handset displays "message sent" it simply means that the message has been received by the SMSC. The two parts of the SMS message, the mobile originated and mobile terminated are independent of each other.

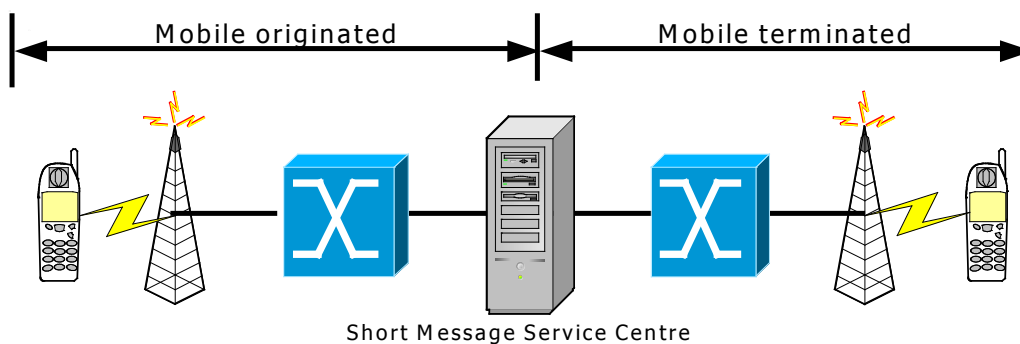


Figure 1 – SMS as store and forward technology

Due to the enormous volume of messages transmitted to the SMSC/MMSC in any given period, messages are routinely deleted by carriers on a daily basis. As is commonly known, electronic files are never completely expunged completely and retrieval of messages is not impossible but extremely difficult and requires expensive technical processes to even locate an identifiable message. The relevance of this point is that the definitions of "stored communication", "passing over" and

“intended recipient” combined to require a communication to be accessible to the recipient and held on equipment operated by the carrier at its premises. In terms of the latter requirement, it is not impossible for a SMS/MMS to continue to be held on carrier equipment in some form.

However, the requirement for the communication to be accessible to the recipient is incapable of being satisfied. Once an end user deletes an SMS/MMS from their device, the message is incapable of being accessed by that person. Importantly, a carrier has no way of knowing whether or not a message has been deleted from an end user’s device. The consequence is that it is impossible for a carrier to know whether the fourth limb of the stored communication definition is satisfied at any point in time.

The practical implications for the carrier include making a judgment on whether or not access to a communication is subject to the new stored communications warrant regime, or whether a search warrant is required pursuant to criminal legislation. This is highly problematic for the carrier, as warrants must be complied with. At the same time, a carrier risks criminal penalties for improper disclosure of communications. The inconsistencies require a judgment call that is impossible to satisfy in a practical sense.

4.6 Application of the legislative framework to instant messaging

The application of the Act to instant messages is even more problematic. Instant message systems do not have any central storage facility. Instead, as set out Figure 2, messages are sent directly between users and the only need for a central system is to be able to identify the Internet Protocol address of the two parties to a message exchange.

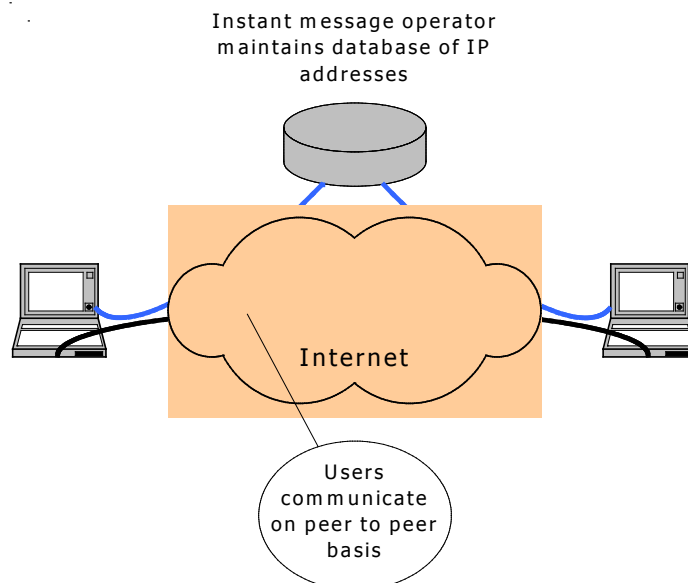


Figure 2 – Peer to peer nature of instant messaging

When a person logs onto an instant message account such as Microsoft Messenger or Yahoo! Messenger, the central database checks to see if any of the person's contacts from their "buddy list" are also signed into the system. Part of the process of signing in, allows the instant message system to identify the Internet Protocol address being used. Once the Internet Protocol addresses are known, each of the users of the instant message system can contact each other directly on a peer to peer basis. That is, there is no stored communication (but nor is there a standard form of communication which could easily be identified under a telecommunications interception warrant).

5 Operation of the law in practice

The introductory comments to this paper noted that operators who are subjected to the access and interception regime are being faced with the increasing difficulty of acting in the spirit, but not to the letter, of the law in matters of law enforcement. Whilst telecommunications is not alone as an industry in operating in a self-regulatory environment, our experience as legal and technical practitioners advising most of Australia's operators at some point has led to the conclusion that there are 3 key problems arising in the sector on matters of law enforcement.

First, some existing practices by law enforcement agencies are based on convention rather than the letter of the law. For example, we are frequently called to advise on warrants which have either expired, not been properly served, or are invalid for other fundamental reasons such as mis-naming the operator on whom it purported to have been served. Frequently, warrants incorrectly cite the grounds on which access is being demanded. For example, s.282 of the *Telecommunications Act 1997* is regularly stated as the basis on which access is being sought by an LEA. This is a legally incorrect ground for access. Section 282 is a provision which permits a person (in this case, a carrier) to disclose information to a LEA if that disclosure will assist in the enforcement of the criminal law and other matters. It operates as one of the exemptions to what would otherwise be an offence by the carrier to the prohibition against disclosure of communications information that is protected by law. It is not a provision which gives an LEA any rights at all to demand information, whether or not under a warrant.

Secondly, the gap between LEA appreciation for the technical limitations of their requests raises a raft of practical issues. We have seen stored communications warrants that have been issued covering periods of over 12 months, seeking all SMSs sent and received by any person in a particular city, containing any or all key words listed in the warrant including (by way of illustration only) "Arab", "building", "suitcase" and "car". Granted that certain combinations of words are likely to satisfy a reasonable suspicion test and may be no doubt critical to identifying and averting serious crimes, there still appears to be a limited understanding of the time and complexity involved for an operator to conduct a search of this nature and present it to an LEA in a meaningful way. As mentioned earlier, SMSCs are purged of SMSs daily to prevent the need for each operator to install a hardware the size of Tasmania to store the

billions of messages that are sent and received from their respective networks.

Thirdly, the level and multiple forms of regulation that permeate every aspect of the telecommunications operator's business – from its contracts with customers to the level of interconnection charges it can impose on other operators – means that the players have an acute awareness and sometimes heightened sensitivity to regulation that is often inconsistent and misunderstood. Take for example the by-product reactions of some law enforcement spokespeople during the recent Haneef proceedings. We saw some of the most senior LEAs in Australia calling for identity checks to be undertaken before SIM cards were sold to consumers. As anyone who has a pre-paid mobile service will attest, a system of pre-paid identity verification has operated in Australia for years, as well as an existing statutory requirement for all operators to provide information about phone numbers and their subscribers to an integrated public number database (IPND). Our experience is that telecommunications operators understand that the nature of the industry requires a form and level of regulation not seen in other sectors, but inconsistent approaches to regulation and continually being made “the fall guys” for the sake of a media grab does nothing to progress the carrier-LEA relationship.

The following examples provide a flavour of the issues that arise for carriers in their access and interception compliance obligations on an almost daily basis:

5.1 Operators receiving stored communications warrants for SMS

Despite the analysis presented above, various LEA have served warrants on mobile operators for the contents of SMS. The practical result of such a warrant is that the operator provides the LEA with the communication content of all SMS for any identified target individual. That is, personnel within the mobile operator's business determine that it is more appropriate to respond to a warrant which may be incorrectly served than it is to decline to fulfil the warrant on the basis that to do so could lead to that individual serving a prison term of up to two years.

5.2 Operators receiving warrants for instant messaging

As set out above, instant messages are peer to peer communications which are not stored (other than on the computers of the users). Nevertheless, operators of instant messaging systems do receive requests for assistance and the Australian branches of the multinational corporations which provide such services may receive warrants. The practical result of the warrant being served is that the operator of the instant messaging system routes messages specifically to a facility so that the messages can be recorded and sent on to the requesting LEA.

5.3 State bodies seeking assistance in contravention of Commonwealth statute

Certain State-based statutory bodies have power under their establishing legislation to demand the production of documents and materials. Despite the

fact that there is an obligation not to disclose material of the form of interception related information under the *Telecommunications Act 1997*, the normal outcome of such requests is that the material is provided to the State body – despite the fact that such inconsistencies should mean that Commonwealth law “trumps” State law by virtue of the Constitution.

5.4 Requests for information or action without a warrant

It is common practice for bodies such as LEAs and public prosecution entities to issue requests for information or action by operators in the absence of a warrant, citing provisions such as s.282 of the *Telecommunications Act 1997* as the head of power. As mentioned previously, this is an exemptions provision and not a standalone head of power. In some cases when the validity of those requests is questioned on this basis, we know of operators that have had s.313 of the *Telecommunications Act* quoted back to them. Section 313 is an “umbrella” obligation that requires a carrier or carriage service provider to give LEAs “such help as is reasonably necessary” to, among other things, safeguard national security. The purposive approach to statutory interpretation appears to have been disregarded by reliance on such a broad power rather than specific provisions of the Act.

6 Discussion

The case studies and the legislative changes lead to a simple question: “Why do the employees of telecommunications operators and the operators themselves, risk prison time to deliver material to LEAs, simply because they are asked?”

It seems to us that the answer to this question must lie in a reasonable risk analysis having been performed by the individual concerned. That is, the telecommunication operator’s personnel take a view that the Australian Communications and Media Authority (**ACMA**) which is responsible for enforcing elements of the *Telecommunications Act 1997* engages in regulatory forbearance when LEAs take decisions that material is required.

This appears to be part of a more general trend which is reflected in the legislative amendments that were introduced in 2006 and which are proposed for 2007. Broadly, this sees the movement of responsibility for law enforcement aspects of the telecommunications legislative and regulatory regime moving from the Department of Information Technology, Communications and the Arts to the Attorney General’s Department. The consequence of this change is dramatic in that the objects of the *Telecommunication Act* form part of the interpretation of that Act when it applies to law enforcement. These objects are drafted to promote the long term interests of end users by strong development and innovation within the telecommunications sector. In contrast, the Act has no objects and is solely devoted to interception issues.

That there has been this shift in regulatory authority reflects government policies since 9/11 in respect of security matters. We do not question the need for this shift

or the relevance of Australia's enforcement agencies. What we do question is the quality of some key elements of legislative drafting in Australia, that has been the core of many of the commercial uncertainties described above.

7 Conclusions

Telecommunications operators in Australia are being increasingly compelled to compromise their strict obligations under the law with a desire to be viewed as co-operative rather than obstructionist with LEAs. Our view is that too many "commercial calls" and "one-off relationship decisions" are made on issues of national security obligations that should be clearly articulated in legislation and in practice. This is an untenable situation and needs to be urgently addressed by a more thorough and thoughtful application of the law by all parties. Regulation of telecommunications for national security purposes is rightly viewed as serious. It should be applied seriously and with the strictest and most robust legal standards.

The social implications of our conclusions are stark. There is an individual expectation that calls will not be intercepted and that communications will not be accessed because, as a matter of law, there is a strict prohibition on such interference. In practice, this strict prohibition has been compromised under the banner of commercial expediency and an over-zealous support of the spirit (but not the letter) of a legislative regime which seeks to provide protections against terrorism and other crimes. If the results of this enthusiasm are a reflection of the inadequacy of parliamentary drafting, then the appropriate course is to redraft the legislation.

References

- Bawa, N. 2006. "The Regulation of the Interception of Communications and Provision of Communication Related Information Act." In *Telecommunications Law in South Africa*, eds. Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Rebyburn. Johannesburg: STE Publishers.
- Bellovin, Steven, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson and John Treichler. 2006. "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP." Washington: Information Technology Association of America.
- Branch, Philip A. 2003. "Lawful Interception of the Internet." Melbourne: Centre for Advanced Internet Architectures, Swinburne University of Technology.
- Del Bianco, Mark C. 2006. "Voices Past: The Present and Future of VoIP Regulation." *CommLaw Conspectus* 14:365-401.
- Drinan, H., N. Fontaine and B. Kesler. 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, C. Besset and B. Aidan. 2004. “Service Aware Intelligent GGSN.” Alcatel Telecommunications Review 1st Quarter 2004:2-10.
- Gidari, Albert. 2006. “Designing the Right Wiretap Solution: Setting Standards under CALEA.” IEEE Security and Privacy(May/June 2006):29-36.
- Gratzer, V., D. Naccache and D. Znaty. 2006. “Law enforcement, forensics and mobile communications.” In Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on.
- Holland, Bradley. 2004. “Overtaking privacy in the telecommunications transit lane.” Privacy Law and Policy Reporter 10.
- Landau, Susan. 2005. “Security, Wiretapping and the Internet.” Security and Privacy Magazine, IEEE(December 2005):26-33.
- Miettinen, Kari. 1999. “Lawful Interception in GPRS/UMTS Network.” Helsinki: University of Helsinki.
- Milanovic, A., S. Srblic, I. Raznjevic, D. Sladden, I. Matosevic and D. Skrobo. 2003a. “Methods for lawful interception in IP telephony networks based on H.323.” In EUROCON 2003. Computer as a Tool. The IEEE Region 8.
- Milanovic, A., S. Srblic, I. Raznjevic, D. Sladden, D. Skrobo and I. Matosevic. 2003b. “Distributed system for lawful interception in VoIP networks.” In EUROCON 2003. Computer as a Tool. The IEEE Region 8.
- Miller, H. G., H. D. Levine and S. N. Bates. 2005. “Welcome to convergence: surviving the next platform change [Internet protocol].” IT Professional 7(3):18-25.
- Nolin, Christopher A. 2006. “Telecommunications as a Weapon in the War of Modern Organized Crime.” CommLaw Conspectus 15(Fall 2006):231.
- Open Mobile Alliance. 2005. “Push to talk over Cellular (PoC) - Architecture.” La Jolla: Open Mobile Alliance.
- Schwaderer, Curt. 2007. “Lawful surveillance systems: Enforcing justice while protecting individual privacy.” In CompactPCI and AdvancedTCA Systems.
- Street, M. D. 2003. “Interoperability and international operation: an introduction to end to end mobile security.” In Secure GSM and Beyond: End to End Security for Mobile Communications, IEE Seminar on (Digest No. 2003/10059).
- Williams, Nigel and Joanne Ly. 2004. “Securing Public Instant Messaging (IM) At Work.” Melbourne: Centre for Advanced Internet Architectures, Swinburne University of Technology.

8

Australia and the ‘War against Terrorism’: Terrorism, national security and human rights¹

Mark Rix

Senior Lecturer, Graduate School of Business, University of Wollongong

Abstract

This paper considers whether in the ‘war against terrorism’ national security is eroded or strengthened by weakening or removing the human rights of the individuals who constitute the polity. It starts with the view that national security is, at its most fundamental, founded upon the security and liberty of the person from criminal and violent acts, including terrorist attacks. Such attacks, and the individuals and groups who perpetrate them, constitute a grave threat to the peace and security of nations the world over and thus endanger the security and liberty of the individuals who make up their populations. Governments are therefore compelled to use the machinery of the state to protect the nation and the individual from these attacks. However, the paper is based on another, equally important, assumption. This is that the defence of national security requires individuals to be protected from the arbitrary exercise of state power even in situations where the state claims to be acting to protect national security and individual security against grave threats such as terrorist acts. The rule of law not only protects individuals from such an exercise of state power by protecting their human rights, in so doing it also protects the peace and security of the nation from excessive and unchecked state power. But what happens when the rule of law is overturned by governments declaring that they are protecting national security from the terrorist threat? Who or what is then able to protect the individual and the nation from the state? This paper will take up these important questions by considering the implications of the anti-terrorism legislation that has been introduced in Australia since September 2001. It will also consider whether Australia’s national security has been enhanced or damaged by this legislation.

Keywords: ‘war against terrorism’, national security, human rights, security and liberty of the person, state power, rule of law

¹ I am grateful to my colleagues Susan Dodds and Luke McNamara for helping me to clarify several of the thorny issues discussed in this paper. Naturally, the usual disclaimers apply.

1 Introduction

This paper will investigate whether Australia requires a new conception of national security that better equips it to meet the challenges it faces in the age of terror than the conventional conception. In the conventional view, a major challenge facing the Government is to balance its responsibility to protect the community from terrorist attack with its equally important responsibility to respect individual human rights and uphold the rule of law. According to this view, however, sometimes the defence of national security requires human rights and the rule of law to be relegated to a much lower priority. Instead, this paper argues that a new conception of national security is required which embeds human rights and the rule of law in national security. On this view, therefore, in defending national security human rights and the rule of law also have to be protected. Put another way, the protection of human rights and the rule of law *is* effectively the defence of national security.

Focusing on two of the most important and far-reaching pieces of anti-terrorism legislation, the paper will consider the exceptional measures contained in Australia's anti-terrorism legislation. These are the ASIO Act (2003) and the Anti-Terrorism Act (No. 2) (2005). The analysis of the exceptional measures will address two separate but inter-related questions: 1) Are the exceptional measures included in the anti-terrorism legislation necessary to protect Australia's national security in face of the terrorist threat? 2) Are there any protections available for the individual and society from abuse of state power when a government weakens the rule of law, thereby diluting the human, civil and political rights it protects, claiming that this is an essential measure to protect national security from the terrorist threat? The exceptional measures include removal of the right to remain silent, reversal of the onus of proof, and the detention in secret of non-suspects merely for questioning (Rix 2006). Moreover, the two Acts to be considered in the paper place tight restrictions on the disclosure of information about cases in which persons are held in custody by the security agencies. Under these circumstances, it is extremely difficult for independent legal representatives to scrutinise and monitor the activities of the security agencies thus impeding them from exercising the right of habeas corpus on behalf of detained persons. They are also prevented from mounting media and advocacy campaigns around such cases. The Government maintains that the exceptional measures provide the Government and national security authorities (including ASIO and the Australian Federal Police) with essential powers for effectively meeting and neutralising terrorist threats (see, for example, Ruddock 2004 and 2005).

2 Australia's national security, the terrorist threat and human rights

Two fundamental assumptions underpin the paper. First is the view that national security is founded upon the security and liberty of the person from criminal and

violent acts, including terrorist attacks. This puts a heavy responsibility on the state, and the government administering it, to take effective measures to protect people, as individuals and as members of social and economic groupings, from threats and acts of this nature. Working from this basic assumption, governments are compelled to use the machinery of the state, and the law and legal system framing it, to take measures to protect individuals, the social and economic infrastructure of society, and the state itself from attacks mounted by terrorist organisations and individuals. However, the paper's second underlying assumption is that the defence of national security requires individuals to be protected from the arbitrary exercise and abuse of state power even in situations where a government claims to be acting to protect national *and* individual security from the threat of terrorism. On this view, the rule of law not only protects the individual from the state, in so doing it also protects the security and freedom of the nation from state repression. In the words of former President of the Israeli Supreme Court Aharon Barak "There is no security without law. Satisfying the provisions of the law is an aspect of national security" (Barak J cited in Kirby J 2005: 328). Legislation which does not respect the rule of law and the human and other rights it protects cannot credibly claim to be able to offer an effective defence of the individual or the nation against threats and attacks by terrorists who have nothing but contempt for these rights and for the rule of law. As Martin Scheinin, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism asserts in his study of Australia's human rights compliance while countering terrorism:

States have a duty to protect their societies and to take effective measures to combat terrorism. States are also obliged, by reason of their international obligations and as emphasized in various documents of the United Nations, including resolutions of the Security Council, to counter terrorism in a manner that is consistent with international human rights law. As stated in the United Nations Global Counter-Terrorism Strategy (part IV) effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing ones. The defence of human rights is essential to the fulfilment of all aspects of a global counter-terrorism strategy (Scheinin 2006: 5; a number of relevant Security Council resolutions will be briefly considered in the following section).

Attorney-General Philip Ruddock, in his 2004 paper 'Australia's Legislative Response to the Ongoing Threat of Terrorism' seemed to be in agreement with the sentiments that were expressed by the Special Rapporteur. In the paper, the Attorney-General asserted that the focus of measures to combat terrorism should be on "creating 'human security' legislation that protects both national security and civil liberties" (Ruddock 2004: 254). Recognising that "[t]he tightening of security will have some effect on certain rights", he assured his readers that "it is our duty to ensure that we employ measures to minimise the impact of counter-terrorism

laws on human rights” (Ruddock 2004: 254). Ruddock also responded to criticisms that the Government’s anti-terrorism “efforts” had failed “to adequately protect our civil liberties” (Ruddock 2004: 255). While these criticisms were based “on the false assumption that counter-terrorism legislation is inevitably at odds with the protection of fundamental human rights”, Ruddock did nevertheless have to admit that “the Government has sometimes compromised on these points to achieve the overriding goal of enacting new laws to combat terrorism” (Ruddock 2004: 255).

Since, September 11, 2001 there has been a substantial increase in the volume of Australia’s anti-terrorism legislation. During its hearing into Australia’s anti-terrorism laws, the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights of the International Commission of Jurists (ICJ) remarked that its attention had been “drawn to the large number of laws enacted since 2002 as part of Australia’s strategy to counter terrorism” (EJP 2006: 1). In an earlier publication, ICJ Australia had pointed out that “[a]s at September 11, 2001, there was in place a patchwork of some 35 pieces of Commonwealth legislation in Australia relating to terrorism, dealing with issues including air navigation, police powers, chemical and biological weapons, criminal offences, hostages, immigration, border protection, intelligence, nuclear non-proliferation, proceeds of crime, telecommunications, and weapons of mass destruction” (ICJ Australia 2004: 1). High Court Justice Michael Kirby has also called attention to the fact that since the attacks of September 2001 “17 items of legislation restricting civil freedoms have been adopted by the federal Parliament” with complementary State legislation also being passed (Kirby J 2004: 226).

According to the Eminent Jurists Panel, Australia is widely regarded and admired “as a country with longstanding democratic practices” in which “[t]he independence of the judiciary, respect for the rule of law, the rights of the accused and an accountable justice system are well established” (EJP 2006: 1). It also noted that both civil society and the media are “active and vibrant”. Taken together all these factors “provide an important protection against the arbitrary use of powers” by the state and its agencies (EJP 2006: 1). However, the EJP also sounded a note of caution:

Members of civil society and the legal community questioned whether many of the new laws were indeed required. They stressed the need to complement counter-terrorism laws with the ability to effectively test them in court for compliance with international human rights standards. Concerns were raised regarding provisions that have introduced broadly defined offences, allowed retrospective application of the law, expanded powers of the executive branch of government and constrained avenues of judicial review and due process of law (EJP 2006: 2).

A number of the issues raised by the Eminent Jurists Panel will be taken up below in the discussion of the exceptional measures that are included in the ASIO Act and the ATA Act (No. 2). These exceptional measures include the executive proscription

power and the detention in secret of non-suspects merely for questioning and intelligence-gathering purposes.

3 Australia's anti-terrorism legislation: review and reality

Like the Eminent Jurists Panel, Martin Sheinin, the UN Special Rapporteur, acknowledged that the need for legislative reform since 11 September 11 2001 had been questioned by “[m]any from civil society”. But, as he points out, while the Australian Government itself acknowledged in a report to the UN Counter-Terrorism Committee in 2003 that the pre-2001 legislative framework for counter-terrorism was adequate and comprehensive—after all, as at September 11 2001, there were already 35 pieces of terrorism-related legislation on the statute books—there had nevertheless been a need to bring the existing legislation into line with UN Security Council Resolution 1373. This resolution calls on States to prevent and suppress the financing of terrorism and to criminalise providing or collecting funds to finance acts of terrorism. There had also been a need to comply with the work of the UN Security Council Al-Qaida and Taliban Sanctions Committee established by UN Security Council Resolution 1267 in 1999. This Committee, amongst other things, maintains and constantly updates (based on information provided by members states) Consolidated Lists of individuals and groups belonging to or associated with Al-Qaida and of groups and individuals belonging to or associated with the Taliban. Under Resolution 1267 all States are obliged “to freeze the assets, prevent the entry into or the transit through their territories, and prevent the direct or indirect supply, sale and transfer of arms and military equipment, technical advice, assistance or training related to military activities, with regard to the individuals and entities included on the Consolidated List” (UN n.d.).

The Special Rapporteur also referred to the 2006 Report of the Security Legislation Review Committee (SLRC) in his report. He noted that the SLRC “was satisfied that separate security legislation, in addition to the general criminal law, was necessary in Australia” (Sheinin 2006: 4; see SLRC 2006: 3). However, unfortunately the Special Rapporteur did not mention several aspects of the SLRC’s report which should have been taken as caveats on the SLRC’s statement regarding the necessity of separate and additional security legislation (several of these same caveats, and for similar reasons, apply to the Parliamentary Joint Committee on Intelligence and Security’s 2006 Review of Security and Counter Terrorism Legislation; see PJCIS 2006). These caveats reveal the difficulties in fully protecting the human rights of Australians in the absence of a Bill or Charter of Rights. They also demonstrate that such an instrument would play an important role in opening up the Government and the law enforcement and security agencies to greater public scrutiny by making them subject to a more effective accountability regime. Before considering these aspects of the report in some detail, some background information on the SLRC and the legislation it reviewed is required.

The independent Security Legislation Review Committee was established by

the Federal Attorney-General on 12 October 2005 with the Honourable Simon Sheller AO QC appointed as Chairman (thus, the Committee was known as the Sheller Committee). The Committee was composed of major stakeholders including the Inspector-General of Security and Intelligence, the Privacy Commissioner, the Human Rights Commissioner, the Commonwealth Ombudsman and a representative of the Law Council of Australia. The latter is “the peak national representative body of the Australian legal profession, representing approximately 50,000 Australian lawyers through its representative bar associations and law societies” (SLRC 2006: 20). The Committee conducted a public inquiry which received nearly 30 submissions and took evidence from 18 witnesses during hearings in Melbourne, Sydney, Canberra and Perth. It reported to the Attorney-General on 21 April 2006 who tabled its report in the Parliament on 15 June 2006.

The SLRC was established pursuant to section 4(1) of the Security Legislation Amendment (Terrorism) Act 2002 (the SLAT Act) as amended by the Criminal Code Amendment (Terrorism) Act 2003. Under Section 4(1) the Attorney-General is required to review “the operation, effectiveness and implications” of the amendments made by the SLAT Act itself, the Suppression of Financing of Terrorism Act 2002, Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002, Border Security Legislation Amendment Act 2002, Telecommunications Interception Legislation Amendment Act 2002 and Criminal Code Amendment (Terrorism) Act 2002 (SLRC 2006: 17). Here is the first caveat on the SLRC’s report. The SLRC was established to review the operation, effectiveness and implications of the anti-terrorism legislation enacted in 2002 and 2003, not the subsequent and even more far-reaching legislation, in particular, the ASIO Act and the ATA Act 2005 which will be considered below. The task of reviewing amending legislation was made even more difficult for the SLRC because, since the enactment of the six amending Acts it was mandated to review “the several amendments they made to other legislation, such as the Criminal Code Act 1995 (Criminal Code), were later further amended” (SLRC 2006: 17). This is a second caveat on the SLRC report, for the complexity and confusion created by the use of amending legislation has been a defining feature of the manner in which the Government has pushed the anti-terrorism legislation through both houses of the Parliament. This has involved

the use of sprawling, omnibus legislation by which multiple Acts are amended in a complex web of interlocking changes within a single amendment Bill, which makes extensive debate and parliamentary supervision difficult; an absence of appropriately argued justification for such significant changes; minimal time for consideration of the legislation by parliamentary committees; and, finally, a determination on the part of the Government to implement its original proposals in the face of parliamentary and community concerns (Hocking 2004: 322).

It is interesting that the SLRC did comment on the limited time available to it for review of the legislation. As well as being granted only six months to conduct the

review (covering, as it pointedly noted, the Christmas/New Year and Easter holiday periods) the Committee had difficulty in reviewing the operation, effectiveness and implications of the “significant amendments” to the relevant legislation because it was required to do so very soon after they had come into effect. Together, these can be taken as a third caveat, for the Committee had very little opportunity to conduct the comprehensive and far-reaching review that was required to ensure that fundamental human rights and the rule of law were being safeguarded in the legislation.

In addition to the above, a fourth caveat, the Committee was concerned with the perplexing and significant issue of which version of the legislative amendments that should have been subject to review. It sought the advice of the Australian Government Solicitor as to whether its examination should be confined to the original text of the amending Acts or broadened to include the amendments contained in other legislation that had been created by the original legislation. Mr Henry Burmester QC, Chief General Counsel of the Australian Government Solicitor advised in this regard that “so long as the review examined the original amendments (in the sense of noting that they had been replaced or amended), it could not be criticised if it took the sensible decision to review the current form of those amendments” (SLRC 2006: 18). The Committee agreed that this would be a “sensible” course of action for it to take but was nevertheless concerned that it would only exacerbate the considerable difficulties it already faced in fulfilling its mandate of reviewing the operation, effectiveness and implications of the specified amending legislation. There were two major difficulties here which together constitute a fifth caveat on its report. First, the Committee did not have access to information about the way in which the law enforcement and security agencies had used the legislation or how the relevant provisions had been interpreted and applied by the courts. Second, and perhaps more significantly, the SLRC had not “itself received confidential briefings about the level of threat of terrorist activity currently faced by Australia” (SLRC 2006: 3). This, however, was an issue on which the Committee undertook to elaborate in its report.

It did so, but only obliquely, in the already cited comments about the difficulties associated with reviewing not only amending legislation but also subsequent amendments to the amending legislation. And it did so again in its remarks on the small amount of time that it had been granted to review the operation, effectiveness and implications of this complex web of amending legislation so soon after its enactment. While these comments are interesting and valuable in their own right, they do not address the more fundamental concern with the secrecy surrounding the level of terrorist threat currently faced by Australia and whether therefore the anti-terrorism legislation provides the Government, and the law enforcement and security agencies it directs, with the resources and means adequate to meet the threat. In other words, the Committee’s comments tells us next to nothing about whether the legislation taken as a complete package is actually necessary to protect Australia’s

national security from that threat or even the precise nature of the threat.

The SLRC also expressed some misgivings about the ASIO Act 2003, but only to point out that its terms of reference prevented it from considering in detail the exceptional measures contained in that legislation. It was noted above that the SLRC was established under section 4(1) of the SLAT Act (as amended by the Criminal Code Amendment (Terrorism Act) 2003) which is headed 'Public and independent review of the operation of Security Acts relating to terrorism'. However, as the SLRC pointed out in its report "Section 4 of the SLAT Act does not refer to what are arguably the most controversial aspects of the security legislation found in Division 3 of Part 3 of the Australian Security Intelligence Organisation Act 1979 (the ASIO Act) as currently amended, and in Divisions 104, 'Control orders' and 105, 'Preventative detention orders' of Part 5.3 of the Criminal Code (SLRC 2006: 22)." These are some of the exceptional measures that will be considered in the next section. For clarification, the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 amended the ASIO Act 1979. In essence, the amendments enable ASIO to obtain a warrant to detain and question persons (who do not themselves have to be suspected of terrorism offences) in order to gather intelligence related to terrorist activity. This ASIO Act was further amended by the ASIO Legislation Amendment Act 2003 to ensure that in planning and executing warrants ASIO has the ability to collect intelligence and information that it regards as necessary to prevent a terrorist act.

The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 (the ASIO Act) that was introduced into Parliament in 2003 was the outcome of a lengthy process of community consultation, inquiries conducted by several parliamentary committees such as the Parliamentary Joint Committee on ASIO, ASIS and DSD (renamed the Parliamentary Joint Committee on Intelligence and Security in late 2005), and wider parliamentary debate. Some minor improvements were made to the bill's original harsh provisions such as those allowing for incommunicado detention, executive proscription and preventing independent legal representation for suspects during detention. But the Government's earlier failure to gain full Parliamentary endorsement of some of the harsher measures it had proposed for inclusion in the SLAT Act, in particular the proscription power, appears to have strengthened its resolve. When first introduced by the Government into Parliament, the SLAT Act had contained provisions enabling the Executive to proscribe so-called 'terrorist organisations' by allowing the Minister (Attorney-General) to issue just such a proscription on his own authority. After community consultation and parliamentary review a compromise was reached whereby "an attenuated form of the power [of proscription] was introduced which allowed provision for the proscription of organizations listed by the United Nations as 'terrorist organisations'" (Hocking 2004: 321). As Hocking notes, however, the Government effectively circumvented the Parliament and challenged its authority by including the power of ministerial (or, executive) proscription in the Criminal

Code Amendment (Terrorist Organisations) Act 2004. But this was not enough, for “[i]n late 2003, the Government introduced further amendments to the newly empowered ASIO Act, seeking stringent secrecy provisions in relation to public disclosure of the implementation of its detention regime and still further expanded interrogation powers” including the doubling of the questioning period to 48 hours if an interpreter had been present at any stage of the interrogation (Hocking 2004: 328).

The ASIO Act gives ASIO the power “to obtain a warrant to detain and question a person who *may have* information important to the gathering of intelligence in relation to terrorist activity” (‘Australian Laws to Combat Terrorism’ n.d.; emphasis added). The Act defines a warrant “issuing authority” as a person appointed by the Minister, who can be a federal magistrate or judge or “another class of people nominated in regulations” (Michaelson 2005: 326). As Christopher Michaelson points out, this act empowers ASIO to “detain people without judicial warrant for up to seven days and interrogate them for up to 24 hours (if no interpreter is present) within that seven-day period” (Michaelson 2005a: 178). Thus, persons can be detained without charge, and do not even have to be suspected of having committed any offence to be taken into custody. While being interrogated, a detainee has to answer all questions and provide all the information or material requested of them. A detainee also has to prove that they do not have the material requested. If the detainee is unable to do so and does not provide the material they can be imprisoned for up to five years. These special detention and questioning powers granted to ASIO had initially been part of the SLAT Act. The SLRC Report notes that the inclusion of these provisions in the ASIO Act “generated extensive debate” which was “in part” about “detention for seven days, removal of the right to silence, some restrictions on access to legal representation, secrecy of interrogation and the extension of the system to non-suspects” (SLRC 2006: 22; see also Michaelson 2005a). After reviewing ASIO’s questioning and detention powers in 2005, the Parliamentary Joint Committee on ASIO, ASIS and DSD recommended that they be continued beyond the sunset period of July 2006 subject to certain conditions. The Joint Committee will review the powers again in 10 years (PJCASIO, ASIS and DSD 2005). In the meantime, the continuation of ASIO’s questioning and detention powers was confirmed in the ASIO Legislation Amendment Bill 2006.

In addition to the above, the ASIO Act specifies a “prescribed authority” who watches over a person held in detention for questioning as a federal magistrate or a member of the Administrative Appeals Tribunal (AAT). The AAT, however, cannot be regarded as a judicial body. Instead, the International Commission of Jurists Australia regards the AAT as a “quasi-judicial body” which lacks the full independence of the judiciary. This is because, with the exception of its presidential members, the members of the AAT are appointed for fixed periods and are therefore “dependent on the favour of the executive if they wish to be reappointed” (ASICJ 2004: 3). It is inferior in this respect to the Special Immigration Appeals Commission (SIAC)

that was established in Britain in the wake of the European Court of Human Rights ruling in *Chahal v. United Kingdom* 1996 (Michaelson 2005b: 137). The AAT is rather more similar to the British ‘three wise men’ body that was superseded by SIAC. In the *Chahal* case, the ECHR ruled that the non-judicial body known as the ‘three wise men’, which up to then had reviewed decisions of the Home Secretary to remove people from England whose presence in England was regarded as “not being conducive to the public good” for reasons of national security, was in contravention of the European Convention on Human Rights (House of Commons 2003). Furthermore, notes Michaelson, “the ‘prescribed authority’ as established in the ASIO Act cannot be considered a ‘court’ or ‘officer authorized by law to exercise judicial power’ within the meaning of Articles 9(3) and 9(4) of the ICCPR [International Covenant on Civil and Political Rights]” (Michaelson 2005b: 137).

The Anti-Terrorism Act (No. 2) 2005 (the ATA Act 2005) was passed into law in December 2005. The “key features” of the ATA Act 2005 include:

- a regime that will enable courts to place controls on persons who pose a terrorist risk to the community
- arrangements to provide for the detention of a person for up to 48 hours to prevent an imminent terrorist attack or preserve evidence of a recent attack
- an extension of the stop, question and search powers of the Australian Federal Police (AFP)
- powers to obtain information and documents designed to enhance the AFP’s ability to prevent and respond effectively to terrorist attack (Ruddock 2005a).

In issuing a control order a court can impose conditions on an individual including a requirement that the person wears a tracking device, a prohibition or restriction on the person talking to other people including their lawyer, and a prohibition or restriction on the use of a telephone or the internet by the person (Walton 2005: 4). As for preventative detention, the police can detain without charge a person who they suspect will carry out an imminent terrorist act or is planning to carry out such an act. They can also hold someone who they suspect “has a ‘thing’ that will be used in an imminent terrorist act” (Walton 2005: 4). The Act allows for a person subject to a control order to be informed of why the restrictions were imposed. However, this “would not require the disclosure of any information that is likely to prejudice national security, be protected by public interest immunity, put at risk ongoing law enforcement or intelligence operations or the safety of the community” with similar conditions applying to an AFP request for variation of a control order (‘Details of Amendments’; attachment to Ruddock 2005).

The ATA Act 2005 also includes an “updated” sedition offence “to cover those who urge violence or assistance to Australia’s enemies” (‘Australian Laws to Combat Terrorism’ n.d.). Commenting on this offence, George Williams points out that “[it] punishes people with up to seven years’ jail not for what they do, but for what they

say, such as if they *urge* another person to forcibly overthrow the constitution or government” (Williams 2006; emphasis added). It includes sweeping bans on free speech and expression and allows for very few defences against the charge of sedition. Williams regards it as one of “worst examples of the history of law-making in the history of the Federal Parliament” and almost without precedent in that “[i]t is hard to think of another example where a law targeting something as fundamental as free speech has been enacted as quickly with as many people from all sides of politics recognising that it needed to be amended even as it was being enacted” (Williams 2006). Chris Connolly remarks that, with the exception of Australia, “no modern democratic nation has used sedition provisions for 50 years” (Connolly 2005: 14). Countries that have repealed sedition laws, or which are in the process of doing so, include Canada, Ireland, Kenya, New Zealand, South Africa, Taiwan, and the United States. In introducing sedition laws, Australia joins China, Cuba, Malaysia, North Korea, Singapore, Syria, and Zimbabwe (Connolly 2005: 14; see also ALRC 2006: Chapter 6, *Sedition Laws in Other Countries*). In response to such criticisms, the Attorney-General requested the Australian Law Reform Commission to conduct a “detailed review” of the crime of sedition. In May 2006, the Commission released its Discussion Paper 71 ‘Review of Sedition Laws’ which called for the removal of the term ‘sedition’ from the Federal statute books and a redrafting of the offences relating to urging force or violence against the government or groups in the community (ALRC 2006). This recommendation has been rejected by the Government.

4 Australia, the war on terror and human rights protection

Why has Australia’s anti-terrorism legislation failed to provide human rights safeguards and why has it with so little inhibition been allowed to subvert the rule of law? Although Australia is a signatory to the International Covenant on Civil and Political Rights (ICCPR), for example, its anti-terrorism legislation such as the ASIO Act and the ATA Act 2005 does not conform with its human rights obligations including those under Article 9 which prohibits arbitrary arrest or detention and under Article 14 on due process of law (Coutts 2006: 40; see also Michaelson 2005b cited above). As the SLRC blandly acknowledges in an unintended response to the question at the opening of this section “Australia has no formal Charter of Human Rights” (SLRC 2006: 3). Such an instrument would serve as a standard against which to assess the validity of anti-terrorism legislation and other legislation impinging on human rights. It would, for example, have allowed the Security Legislation Review Committee to be more adventurous in its analysis and critique, and to be more courageous in formulating the recommendations it provided arising from the review of the legislation. The UN Special Rapporteur has expressed his concern that “Australia does not have domestic human rights legislation capable of guarding against undue limits being placed upon the rights and freedoms of individuals” (Scheinin 2006: 5). While he acknowledges that the “Government of Australia points to a robust constitutional structure and framework of legislation capable of

protecting human rights and prohibiting discrimination” the absence of domestic human rights legislation “is an outstanding matter that has been previously raised by the Human Rights Committee in its observations on Australia’s reports under the International Covenant on Civil and Political Rights” (Scheinin 2006: 5).

According to George Williams, for many countries with a written constitution like Australia “constitutional development in the second half of the 20th century was dominated by concepts of human rights...Canada and South Africa gained Bills of Rights while the United States saw an existing Bill of Rights expanded through judicial interpretation” (Williams 2001: 782; see also Williams 2003 and 2004 and Nicholson 2005). In countries such as New Zealand and the United Kingdom that do not have a written constitution “international human rights standards were incorporated into domestic law through statutory Bills of Rights” (Williams 2001: 782). The Eminent Jurists Panel has pointed out that Australia has yet to enact federal legislation incorporating international standards into national law, a move which “would help to establish a clear human rights framework based on international standards” (EJP 2006: 3). For Amnesty International Australia, these standards “constitute the bare minimum necessary to protect the safety and integrity of individuals from abuse of power” (AIA 2005: 5-6). Greg Carne points out that UN human rights bodies, such as the High Commissioner for Human Rights, the Commission of Human Rights, the Secretary-General, the Secretary-General’s Policy Working Group on the United Nations and Terrorism, amongst many others, have long advocated a “more holistic approach” to human rights to ensure that measures to counter terrorism are consistent with human rights values and the obligations they entail (Carne 2004: 543). Australia also is not a party to binding international human rights instruments. A good example of such an instrument, even if it is not directly applicable in the Australian context, is the European Convention on Human Rights (and its five protocols) to which many European countries are party the United Kingdom included. The Convention enables the citizens of European countries to appeal to the European Court of Human Rights and seek redress if they believe that the laws of their own countries are in breach of the Convention (just as in the Chalal case cited above) (Nicholson 2005: 3).

As seen above in the examination of the Security Legislation Review Committee’s review of Australia’s anti-terrorism legislation, it is hard to gauge whether the legislation has been effective in protecting Australia from terrorist attack. Indeed, for those Australians who are not members of the Federal Cabinet or the law enforcement agencies and security services it is an unanswerable question. This is because of the secrecy surrounding the issues of whether Australia currently faces a terrorist threat and, if so, the nature and imminence of that threat. In view of this secrecy, little can therefore be said in an informed or sensible way about any terrorist threat that Australia may face in the future. It is thus almost impossible to determine whether the legislation is actually required to protect Australia’s national security from the threat of terrorism. This is more than a little unsettling in the light of claims

made by US President Bush and his allies, including the Howard Government, that the 'war on terror' or 'war against terrorism' will either be of "uncertain duration" or "go for years" (see, for example, Power 2007 and ABC 2007). This means that counter-terrorism measures, like the exceptional provisions included in Australia's anti-terrorism legislation, will also be of uncertain duration or go for years. To be sure, national security is conventionally and rightly regarded as being based upon the security and liberty of the person from criminal and violent attacks, including terrorist acts. But, beyond this, the conventional view also holds that there are times when the protection of national security requires human rights and the rule of law to be given a lower priority. This gives rise to a significant shortcoming with this view of national security, namely, its strong tendency to relegate the security and liberty of the person to a secondary consideration after state security.

If the volume of anti-terrorism legislation and the measures included in it are anything to go by, then the Australian Government has certainly not been backward in using the machinery of the state to protect the country and its people from the threat of terrorism (whatever the actual nature of that threat happens to be). It has also not been backward in privileging state security over human rights and the rule of law. Indeed, in these respects its diligence is to be commended. But, if national security is also regarded as being just as fundamentally based on the security and liberty of the person from the arbitrary exercise or abuse of state power then the legislation would appear to be an abject failure. In the war on terror, as in any other armed conflict or type of war, national security cannot be fully protected by giving priority to the security and liberty of the person either from terrorist attacks or from the arbitrary exercise or abuse of state power. These are two indivisible and absolutely equal aspects of national security. Legislation such as Australia's anti-terrorism laws, therefore, which does not respect the rule of law and the human and other rights it protects cannot credibly claim to be able to offer an effective defence of the individual or the nation against threats and attacks by terrorists who have nothing but contempt for these rights and for the rule of law.

5 Conclusion

Since September 11, 2001 the Australian Government has introduced a whole raft of anti-terrorism legislation which it claims is needed to protect the country and its citizens from terrorist attack. This legislation includes the ASIO Act and the ATA Act 2005 both of which contain exceptional measures diluting or removing established rights and liberties and seriously weakening the rule of law. They thus fail a crucial test when the notion of national security is extended beyond the narrow, conventional view which holds that national security is based on the security and liberty of the person from criminal and violent acts including terrorism. On this view, sometimes the defence of national security requires human rights and the rule of law to be relegated to a much lower priority. This can lead to the privileging of state security over the security and liberty of the person. When the conventional view

is widened to encompass the security and liberty of the person from the arbitrary exercise or abuse of state power the anti-terrorism legislation clearly does not protect Australia's national security and even effectively undermines it. The absence of a Bill or Charter of Rights has left Australians highly vulnerable to arbitrary and excessive state power. Not only is such an instrument urgently required, so also but even more fundamentally is a new conception of national security that will help to ensure that the country's national security is fully protected in the age of terror. A conception of national security which includes the security and liberty of the person from terrorist attack and from state repression as its two indivisible and absolutely equal aspects would go a long way to providing such protection.

References

- ABC (2007) 'War on terrorism will go on for years: PM'. ABC News Tasmania. July 15. Available at: <http://www.abc.net.au/news/stories/2007/07/15/1978787.htm>
- Amnesty International Australia (2005) Submission to the Parliamentary Joint Committee on ASIO, ASIS and DSD regarding the Inquiry into the Operation, Effectiveness and Implications of Division 3 of Part III of the Australian Security Intelligence Organisation Act 1979. March. Available at: http://www.amnesty.org.au/Act_now/campaigns/human_rights_and_security/submissions
- Australian Laws to Combat Terrorism (n.d.) Available at <http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D49EA90CA256FAB001BA5EA?OpenDocument>
- Australian Law Reform Commission (2006) Discussion Paper 71: Review of Sedition Laws. Available at: <http://www.austlii.edu.au/other/alrc/publications/dp71>
- Carne, G. (2004) 'Detaining Questions or Compromising Constitutionality? The ASIO Legislation Amendment (Terrorism) Act 2003'. *University of New South Wales Law Journal*. 27(2): 524-578.
- Connolly, C. (2005) 'Five key facts on sedition'. *Human Rights Defender Special Issue: The Anti-Terrorism Bill (No. 2) 2005*. November/December: 14-16
- Coutts, L.A. (2006) 'A short review of the various Acts of the Federal Parliament that constitute what might loosely be called "anti-terrorist" legislation'. International Commission of Jurists Australia. 1 November. Available at: http://www.icj-aust.org.au/images/stories/documents/061101_-_L_A_Coutts_A-T_Legn_paper.pdf
- Eminent Jurists Panel (EJP) on Terrorism, Counter-Terrorism and Human Rights (an Initiative of the International Commission of Jurists (2006), 'Eminent Jurists Panel concludes Australia hearing on counter-terrorism laws, practices and policies: Press Release'. 17 March 2006. Available at: <http://www.icj-aust.org.au/>

- Hocking, J. (2004) 'Protecting Democracy by Preserving Justice: "Even for the Feared and the Hated"', *University of New South Wales Law Journal*. 27(2): 319-338.
- House of Commons. (2001) Select Committee on Home Affairs – Appendices to the Minutes of Evidence. Appendix 16 'The Special Immigration Appeals Commission (SIAC)'. <http://www.publications.parliament.uk/pa/cm200102/cmselect/cmhaff/351/351ap20.htm>
- International Commission of Jurists Australia (2004) 'Human Rights and Terrorism: Legislative and Policy Responses to Terrorism Post September 11 in Australia', ICJ Biennial Conference, 27-29 August 2004. Available at: <http://www.icj-aust.org.au/>
- Kirby J, Michael (2005) 'Terrorism and the Democratic Response 2004', *University of New South Wales Law Journal*. 28(1): 221-244.
- Michaelson, C. (2005) 'Antiterrorism Legislation in Australia: A Proportionate Response to the Terrorist Threat?' *Studies in Conflict and Terrorism*. 28: 321-329.
- Michaelson, C. (2005a) 'Security Against Terrorism: Individual Right or State Purpose?'. *Public Law Review*. 16: 178-182.
- Michaelson, C. (2005b) 'Derogating from International Human Rights Obligations in the "War Against Terrorism"?—A British-Australian Perspective'. *Terrorism and Political Violence*. 17: 131-155.
- Nicholson, A. (2005) 'The Role of the Constitution, Justice, the Law, the Courts and the Legislature in the Context of Crime, Terrorism, Human Rights and Civil Liberties'. An address to the Post-Graduate Student Conference, Post-Graduate Criminology Society, University of Melbourne. 4 November. Available at <http://www.mpso.unimelb.edu.au/mpso/media/transcripts>
- Parliamentary Joint Committee on ASIO, ASIS and DSD (2005) Review of Division 3 Part III of the ASIO Act 1979—Questioning and Detention Powers. Available at: http://www.aph.gov.au/house/committee/pjcaad/asio_ques_detention/fullreport.pdf
- Parliamentary Joint Committee on Intelligence and Security (2006) Review of Security and Counter Terrorism Legislation. Available at: <http://www.aph.gov.au/house/committee/pjcis/securityleg/report/report.pdf>
- Power, S (2007) 'Our War on Terror'. *The New York Times*. July 29. Available at: <http://www.nytimes.com/2007/07/29/books/review/Power-t.html>
- Rix, M (2006) 'Australia's Anti-Terrorism Legislation: The National Security State and the Community Legal Sector'. *Prometheus*. 24(4): 429-440.
- Ruddock, P (2004) 'Australia's Legislative Response to the Ongoing Threat of Terrorism', *University of New South Wales Law Journal*. 27(2): 254-261.
- Ruddock, P (2005) 'Government Enhances Anti-Terrorism Bill (No. 2) 2005'. Media Release 222/2005. 1 December. Available at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases

- Ruddock, P. (2005a) 'Passage of Anti-Terrorism Bill (No. 2) 2005. Media Release 230/2005. 7 December 2005. Available at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases
- Scheinin, M (2006) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Australia: Study on Human Rights Compliance While Countering Terrorism. Available at: <http://daccessdds.un.org/doc/UNDOC/GEN/G06/155/49/PDF/G0615549.pdf?OpenElement>
- SLRC (2006) Report of the Security Legislation Review Committee. June. Available at: [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](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)
- 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. Available at <http://www.un.org/sc/committees/1267/consolist.shtml>
- Walton, M. (2005) 'The Anti-Terrorism Bill (No. 2) 2005: An Overview', *Human Rights Defender Special Issue: The Anti-Terrorism Bill (No. 2) 2005*. November/December: 3-5
- Williams, G (2001) 'Human Rights and the Second Century of the Australian Constitution', *University of New South Wales Law Journal*. 24(3): 782-791.
- Williams, G. (2003) 'Australian Values and the War against Terrorism'. National Press Club Telstra Australia Day Address. 29 January.
- Williams, G (2004) *The Case for an Australian Bill of Rights: Freedom in the War on Terror*. UNSW Press.
- Williams, G. (2005) 'Jumping the gun on terror'. *The Age*. 27 October.
- Williams, G. (2006) 'Speak up in defence of free speech'. *Sydney Morning Herald*. May 30.

9

Panel session: The case for detention without charge in suspected terrorism cases in Australia

Nick O'Brien

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

Abstract

This paper is the introduction to a more detailed referenced paper, currently in draft form, which discusses the need for detention without charge in terrorist cases in Australia. This document is intended for panel discussion. The paper examines the way that terrorism has changed in the past decade and concludes that detention without charge is needed in terrorist cases in Australia because of the exceptional problems posed by terrorism and counter terrorism. It is also argued that safeguards need to be imposed to ensure that human rights are protected as far as possible.

Keywords: detention, suspected terrorists, terrorism, powers

- 1 Terrorism has changed both in its complexity and violence over the last decade. This change has largely been because of Al Qaeda (AQ) and associated groups. The transformation has manifested itself in a number of different ways.
- 2 AQ related terrorists have a desire to kill as many people as possible. Early indications of this desire was evidenced with the attacks on the Embassies of the United States of America in Dar es Salaam, Tanzania and Nairobi, Kenya on 7th August 1998. Over 300 people were killed in these bombings. Prior to these incidents mass casualty attacks were rare, although some 270 people were killed on 21st December 1988 when Pam Am flight 103 was bombed over the Scottish town of Lockerbie. The Lockerbie attack, however, differs from AQ related attacks as it is likely that it was a State sponsored action rather than one perpetrated by a non-state terrorist group.
- 3 Suicide terrorism has become increasingly popular with terrorist groups, especially those groups that empathise with AQ. The phenomenon of suicide terrorism in modern times began in 1983 with attacks on the US and France in the Lebanon, but has been increasingly used over the past decade in a number of countries including the US, UK, Spain, Iraq, Russia and Afghanistan.
- 4 It is known that AQ desires to use Chemical, Biological, Radiological and Nuclear (CBRN) weapons against its enemies. This is one of the most disturbing facets of 21st century terrorism and some experts consider that a radiological attack is likely to happen in the short to medium term.
- 5 In most cases authorities or third parties can negotiate with terrorist groups, witness the Israel/Palestine dispute, Irish terrorism in the UK, the Basque nationalist dispute in Spain and the situation in Sri Lanka with the Liberation Tigers of Tamil Eelam (LTTE). It would be difficult to negotiate with AQ, although the US government shows little sign of wanting to begin that process.
- 6 Terrorism is now global in nature rather than being confined to a particular country. AQ has links in over 60 countries and terrorist investigations against AQ related groups will always involve at least one other country and often many more. This brings with it the complexities of other countries' legal systems as well as different time zones and languages.
- 7 With the internationalisation of terrorism comes this issue of translating documents and providing interpreters for prisoners who may not be able, or willing, to speak English. Ideally both interpreters and translators should have some vetting to ensure the confidentiality of the information with which they are dealing. Good translators and interpreters are in short supply and may have to be flown in from other cities.
- 8 As well as the change in terrorism, terrorist groups are also taking advantage

of the sophistication of Information and Communication Technology (ICT). Arrested persons could have information on mobile phones, Personal Digital Assistants (PDAs), computers, cameras as well as a variety of media including compact disks and USB sticks. This information will need to be examined by police officers. This examination is a complex process as computers can contain as much information as is found in a library. Additional complications will occur if the information is encrypted or steganography is used. If suspected terrorists make use of internet cafés, it may be necessary to seize and examine all the computers in the café.

- 9 Premises that are suspected of having been used by terrorists should be forensically searched. Police officers should be looking for items as small as a SIM card or USB stick which can be concealed easily. In one case in the UK, police took six weeks to search one address, although this was the 'bomb factory' in Beeston used by the London bombers of 7th July 2005. It would not be unusual in the UK for police to take 2 weeks to search premises suspected of having been used by terrorists.
- 10 The issue of Australia being a target for AQ or related groups is important. If Australia is not a target for AQ or related groups then extraordinary powers will not be needed. However it is apparent that Australia is a target for AQ, indeed Australia has been mentioned a number of times by senior AQ leadership, including Ayman al Zawahiri and Usama bin Laden.
- 11 The issue of human rights needs consideration when considering detention without charge. In 1948 the United Nations (UN) adopted and proclaimed the Universal Declaration of Human Rights, Article 3 of which states, 'everyone has the right to life, liberty and security of person.' Other Human Rights declarations have similar provisions to the UN declaration of Human Rights. The European Union (EU) Convention for the Protection of Human Rights and Fundamental Freedoms protects the right to life (Article 2), and the right to liberty and security (Article 5). The rights set out in various human rights provisions cannot be absolute and there will be occasions when the rights are not compatible with each other. Governments must make decisions on when one right overrides another, for example when the right to life overrides the right to liberty or the right to privacy.
- 12 This paper will examine the way that terrorism has changed and will conclude that police need to be able to detain people suspected of having been involved in terrorism without charge for at least 28 days. Extraordinary situations need extraordinary laws. The detention should be judicially sanctioned after 48 hours and any magistrate or judge should only be able to grant further periods of detention if they are satisfied that police are dealing with the case expeditiously and that there is a need to further detain the suspect for the

purpose of questioning him/her or further examining any seized evidence or that it is reasonably believed that evidence is about to be obtained which may be relevant to the case. The powers should have a 'sunset' clause and should be examined by parliament annually. The use of such legislation requires as much transparency as possible. Whilst it would not be prudent to release all details of investigations to the public as there will be matters of national security, classified documents and the danger of informing terrorists of police/ASIO tactics, the legislation would need independent oversight. A senior judge should be appointed to report to parliament on the use by police, ASIO and other agencies with a law-enforcement remit that covers terrorism, of the use of all counter terrorism legislation. It should be illegal for police, defence lawyers or any third party to disclose details of the case, including interview transcripts during this period as trial by media serves neither the interests of the arrested person nor the interests of justice.

- 13 As stated, modern terrorism is an extraordinary phenomenon and police need extraordinary powers to deal with suspected terrorists. Involvement of the judiciary, both to allow continued detention and to report to parliament, is necessary to reassure the public that the human rights of arrested persons are being considered.

10

The benefits and concerns of public data availability in Australia: a survey of security experts

Roba Abbas

Graduate, School of Information Systems & Technology, University of Wollongong

Abstract

This paper gauges the attitudes of security experts in Australia with regards to public data availability on critical infrastructure protection (CIP). A qualitative survey was distributed to a individuals considered experts in CIP-related research in Australia, in order to address the censorship versus open access debate concerning public data. The intention of the study was to gain an insight into the perceived benefits and threats of public data availability by security experts, and to provide the basis for a security solution to be utilised by the Australian Government sector (at all levels). The findings however can also be applied to other data supplying agencies. This includes the identification and assessment of the technical and non-technical security mechanisms that can be enforced to protect sensitive public data elements that reveal information about Australia's critical infrastructure.

Keywords: critical infrastructure, critical infrastructure protection (CIP), public data, security mechanisms, security

1 Introduction

Critical infrastructure protection (CIP) refers to safeguarding essential services from harm. CIP has gained recognition as a priority area on the national security agendas of many countries in recent years, most notably Australia, due to events that have compromised the critical infrastructure (CI) of other nations. The importance of the CIP process is evidenced extensively in the related literature, where the major phases of the process are discussed. Traditionally, the CIP focus is on the three major stages of vulnerability identification, risk assessment and risk management. A study conducted by Breeding (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, thus posing a threat to CIP.

The primary aim of this study was to raise awareness with respect to the censorship versus open information access debate, which is presently a prominent issue. Of great importance is to deliberate on whether certain CI-related information should be restricted from the public arena in the interest of national security, through a survey of security experts in Australia.

The primary objective of the survey is to gauge the attitudes of the experts with regards to the public data availability dilemma, a dilemma that is conflicted between whether public data should be restricted from public availability or be freely available. Public data related to critical infrastructure (CI) provide details about the characteristics of the CI, and in some instance can reveal sensitive information that can compromise the CIP process.

A qualitative survey was distributed to individuals considered experts in CIP-related research within Australia. Due to the vast and unstructured nature of public data availability, it is evident that many components and aspects of the protecting public data must be considered and a multi-faceted security solution must be devised, based on non-technical and technical mechanisms.

The solution provided throughout this paper is based on the outcomes of the survey, which highlights the need to evaluate alternative security mechanisms, and determine a possible restriction process through the use of a stakeholder matrix. The solution offered is focused on providing practical tools and recommendations that can be applied by government agencies and other data supplying bodies in Australia to assist in protecting CI from the negative implications associated with public data availability.

2 Background to the study

Critical infrastructure (CI) are the essential services that contribute to the stability and security of a country (Chakrabarty and Mendonca, 2004; Rinaldi et. al., 2001). A comprehensive listing of critical infrastructure includes energy, banking/

finance, water, transportation, agriculture, health and emergency, information and communications, storage and transportation, government, law and order, and cultural services (Breeding, 2003; Chakrabarty and Mendonca, 2004; Scholand et. al. 2005). A standard, global definition of critical infrastructure is not available; rather, each respective country determines their critical categories independently, based on the relative importance of each infrastructure item.

Critical infrastructure protection refers to safeguarding the identified services from potential harm, including physical and/or electronic attacks (ASIO, 2006). Although minor variations exist regarding the specific phases of the CIP process, it is widely agreed that the typical steps encompass vulnerability assessment/scanning, risk assessment, and risk management (Luijff and Klaver, 2004; Jones et. al., 2003). The CIP process is a crucial consideration today, particularly due to the prevalence of national security issues as a result of global events, including 9/11 and the Bali bombings.

CIP has been a global concern since the Cold War. However, the issue has gained increased exposure in Australia since the incidents of Y2K, September 11, 2001 and Bali, 2002 (Luijff and Klaver, 2004; Emergency Management Australia, 2003).

Additionally, the importance and increased use of the Internet and Information and Communication Technologies (such as biometrics, database processing, geospatial information exploitation, video processing and visualisations) have amplified the risks on critical infrastructure (Popp et. al., 2004). These technologies provide outlets for data/information exchange, and have simplified the ability to transmit data. Of particular importance to this research is the exchange of 'sensitive but unclassified' public data; data that on its own may be considered unclassified, but when combined may reveal previously unobvious or revealing patterns, which may prove harmful (Thuraisingham, n.d.). Access to such information does serve positive purposes, but can also expose the weaknesses of particular CI, thereby potentially compromising national security efforts if the data is applied maliciously.

An introductory study into the consequences of public data availability on critical infrastructure states that there is an increase in the education levels of the individuals/groups attempting to penetrate critical services (Breeding, 2003). In particular, their use of technologies, and the availability of certain tools, has become progressively sophisticated, allowing room for the collection, use and duplication of information. These concepts are supported by authors such as Weinmann (2006), who asserts that the Internet offers a vast repository of data that may potentially be exploited, and be used to compromise the CIP process, and consequently undermine national security.

The amalgamation of the abovementioned factors has resulted in, or prompted the need for national security to become a major global concern. While there are current government and research initiatives in place focussed on CIP and national security, inadequate attention is paid the notion public data availability in Australia

as a fundamental consideration in the CIP process. Furthermore, it is evident that the benefits of providing and accessing CI-related information online are generally promoted, whereas the negative implications are often ignored. The focus of CIP efforts, to date, have been on the establishment of risk assessment and management strategies, thus reinforcing the need for perceiving CIP from an alternative, but equally significant viewpoint.

This paper will attempt to address the public data availability issue through a survey of individuals considered experts in the CIP field. The study will focus on whether the experts are aware of the apparent threat, and will document the opinions of the individuals, in addition to possible solutions to the identified dilemma.

3 Critical infrastructure protection (CIP) survey

The *Critical Infrastructure Protection Survey* was distributed in hardcopy, at the National Security Technology Conference (21 September, 2006) and also subsequently online. The primary objective of this survey was to discuss issues relating to public data availability in Australia. Of great importance was to determine and gain an appreciation of the public data availability situation, as perceived by security experts. A key factor was to provide an outlet for security experts, researchers and interested parties who are knowledgeable about CIP to communicate their concerns and attitudes, and assist in providing suggestions to solve the public data availability dilemma. This dilemma is centred on the debate of whether public data concerning Australia's critical infrastructure should be restricted from the public domain to ensure that high levels of security are maintained, and that critical infrastructure are not compromised.

An additional objective of this research was to develop a solution using both technical and non-technical security measures. It is clear that the required solution must offer equal benefits to the four distinct community member groups or stakeholders within the Australian community, so as to ensure that a particular stakeholder is not disadvantaged in terms of public data access. The stakeholders include Australian Government agencies, operators of critical infrastructure, educational institutions and research networks, and the general public (citizens).

4 The profile of survey respondents

The qualitative survey yielded twenty-one security expert responses, almost half of which came from individuals employed by the government sector. With respect to the response rate, the survey was primarily focused on qualitative responses to public data availability concerns and the establishment of a practical solution. Therefore, it must be emphasised that the number of responses received was not a limiting factor to the study.

The collective profile of survey respondents reveals a heavy reliance on the use of free public data, or a combination of both free and purchased data. An interesting observation is that not one individual (organisation) depended solely on purchased

public data; a majority of the respondents found that free public data is beneficial for their purposes and in many instances is sufficient for their use.

In terms of day-to-day uses of critical infrastructure data, over half the respondents utilise public data to conduct risk assessment/risk management activities. Additional uses include government intelligence purposes, business intelligence purposes, service provisioning, Customer Relationship Management (CRM), navigation, construction, supporting response agencies with geospatial information, and research (tertiary education) purposes.

The overall profile of the respondents revealed that the group is knowledgeable concerning public data use, and that the data is beneficial for accomplishing daily tasks. Consequently, such information provided the foundations for determining the perceived benefits and concerns of public data availability in Australia, and working towards a solution to reach a balance between restricting data from the public domain and openly providing access.

5 The benefits and concerns of public data availability

Security experts reinforce the need for a balance between data accessibility and restricting access to data. The survey responses generally indicate that the difficulty in this situation stems from the fact that public data availability can present both positive and negative consequences, depending on how the data is applied.

The respondents felt that the benefits accruing from public data availability include promoting community trust, allowing immediate responses in time-critical situations, and assisting in the completion of daily tasks in specific occupations. The use of public data for such applications is crucial; therefore, the security experts generally maintained that it would be unwise to restrict access to the relevant datasets in such situations.

A number of security experts felt that community members have a basic right to access information concerning their surroundings and community. According to a respondent in the government sector, encouraging the concealment of basic community data and enacting harsh restrictions will inevitably result in Australia becoming a “secretive, scared society”, which is a disagreeable effect. An additional point raised was that CI-related data should be publicly accessible “to ensure that governments and infrastructure providers are not relying on security through obscurity.” Trust is an imperative factor in this situation, particularly in view of sustaining a positive relationship and level of transparency between the Australian Government and citizens.

Certain applications, such as emergency management, rely on the transfer and exchange of CI-related data in a timely fashion. A common notion expressed in the survey is that in such applications, direct data access is essential. Public data can therefore aid with activities including continuity planning, evacuation, infrastructure protection, and emergency management for incidents, such as earthquakes, cyclones, tsunamis, bushfires, infrastructure disruptions, and terrorist attacks.

Additionally, the survey revealed that the majority of respondents rely on public data in their respective industries to accomplish daily tasks. Public data access is beneficial in these situations, and increases safety in particular occupations. For instance, a security expert in the construction industry maintained, “as a structural engineer, information such as ground levels, location of buildings, location of electricity, water, gas, etc is critical to the safe design of buildings and infrastructure.” Therefore, access to relevant CI-data, regardless of sensitivity, is required.

Despite these positive aspects, the situation is complicated due to the potentially devastating implications of public data availability, which encourages that the issue of data restriction be considered in order to minimise the existing threats. The concerns relating to public data availability include impacting on national security efforts (and therefore CIP), facilitating other forms of misuse, and affecting the privacy and confidentiality of individuals. These concerns are further explained.

The major concern identified regarding public data availability was the potentially damaging effects on national security and CIP programs, more specifically the use of public data for aiding in terrorist-related activities. As a survey respondent noted “access to data should be well-controlled to minimise the possibility of use by foreign and domestic adversaries”. This thought is shared by other experts, one of which claims “if potential terrorists can access good quality data over the Internet, this can eliminate the need for on-site reconnaissance, which in turn eliminates the opportunity for the behaviour to be noticed, investigated, and attacks disrupted.” Disregarding this concern can result in widespread and immeasurable physical and psychological consequences.

The concerns associated with public data availability are not limited to terrorist-related activities. Security experts expressed that CI-related public data can aid other forms of misuse and offences, with consequences such as increased crime, services disruption, vandalism, identity theft/fraud and obtrusive telemarketing.

Privacy and confidentiality are also key concerns in this discussion. While the data of interest to the research is CI-related, a number of respondents felt that personal privacy is an additional concern, which introduces the ‘personal safety’ dimension to the study. This is an important area for future research.

Therefore, public data availability presents positive and negative implications, although a government official responded that open access to data results in “CONCERNS ONLY”. Similarly, a respondent in the education industry claimed that there were “no major benefits”, as the positive aspects of public data availability are somewhat overshadowed by the potentially devastating damage. However, the majority of respondents feel that strict censorship and data restriction is not a viable option.

A common thread in the survey responses is that information should be available on a “need-to-know basis”, to the appropriate personnel who require the data for carrying out tasks that are advantageous in some way. That is, “the TRADE-OFF between what one needs to have to do their work well, and what needs to be

kept sensitive because it may be used against a nation” must be managed. This is based on the concept that data should not be made available to individuals with no “legitimate” purpose to access it. Legitimate, in this instance, refers to whether an individual can justify that the data accessed will be used positively.

6 Achieving the balance: the public data availability solution

A notable outcome of the survey is that data should only be accessed for “legitimate” reasons. While in theory, this argument is seemingly valid and rational, in practice it is difficult to accomplish. For instance, a number of important questions emerge that require further thought:

- 1) What CI-related data elements will be available to certain individuals?
- 2) What conditions define a “legitimate” purpose?
- 3) How will the process as a whole be enforced?

The basis for a solution utilising non-technical and technical security mechanisms is put forward based on the survey results, providing practical answers to these questions.

An important outcome is the introduction of a stakeholder matrix, which is a non-technical method that can assist in establishing the sensitivity of CI-public data elements. The stakeholder matrix provides a sensitivity-based grading system that determines the relative sensitivity of CI data elements, and recommends who should be granted access to that particular element. The underlying concept behind the stakeholder matrix is to clearly outline the three grades that can be assigned to a data element. The first grade is ‘unclassified/public’ defining that a data element can be accessed by any individual; the second grade is ‘restricted’ meaning that only certain stakeholders are granted access and the final grade is ‘classified/private’ indicating that a data element cannot be publicly accessed under any circumstance.

The recommendation with respect to such a matrix is that it be used by data supplying agencies and bodies to decide which data elements may require censorship or restricted access. A sample matrix, based on the findings of the survey, is provided in Figure 1. The diagram depicts a possible classification system to be used as the foundation of the proposed public data availability solution. In its present form, the matrix can be used as a guideline; however, it is suggested that an expanded matrix be devised containing a comprehensive list of CI-related data elements and a similar analysis be performed by any agency that makes CI data available to the public.

The grade assigned to each specific data element in the matrix is based on whether security experts felt that the particular element should be available to the respective stakeholder. For example, if more than 66 percent of security experts felt a data element should be available, an ‘unclassified’ grade is assigned; if between 33 to 66 percent of security experts believe a data element should be available, a ‘restricted’ grade is assigned and if less than 33 percent of security experts believe it should be available, a ‘classified/private’ grade is assigned.

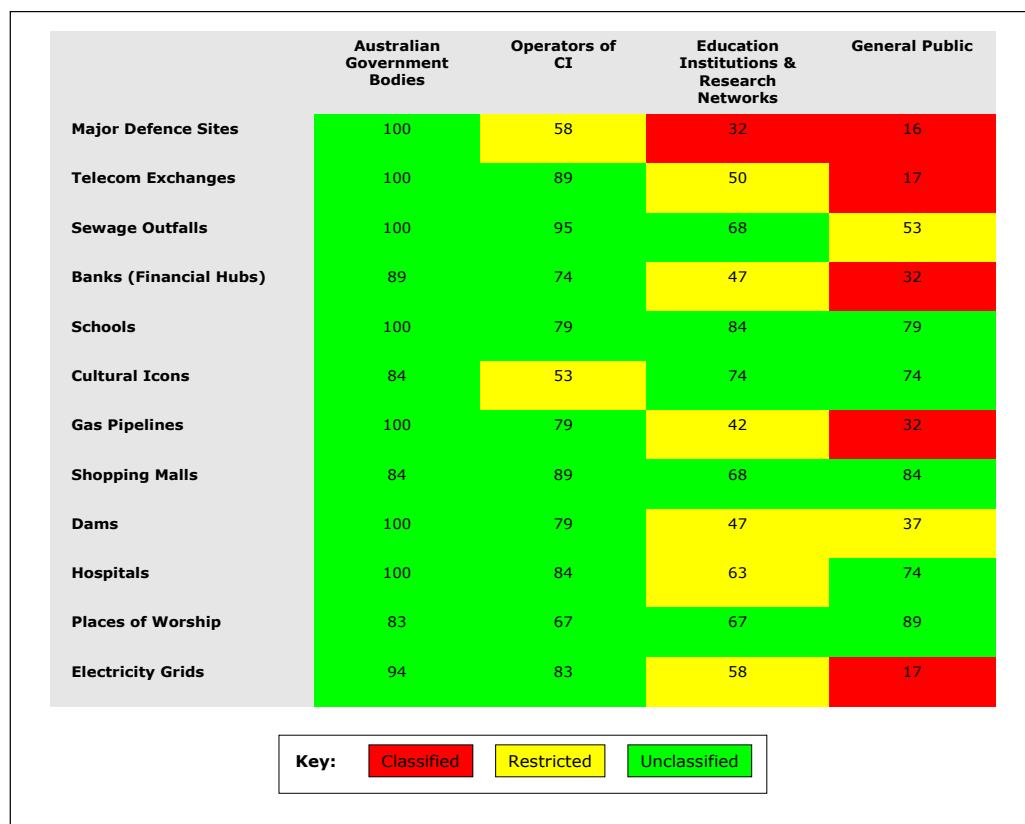


Figure 1. Data Sensitivity Stakeholder Matrix

The stakeholder matrix is a fundamental concept that will form the basis or foundation of any public data protection campaign, and is currently a missing element from the censorship versus open access debate. The survey reinforced the idea that this mechanism should be supported by additional security techniques, both non-technical and technical in nature.

Non-technical security mechanisms refer to public data protection tools that do not require the use of technology to be accomplished. Survey respondents feel that non-technical security techniques can be beneficial in public data protection initiatives, the most appropriate being:

- Legal and licence agreement containing conditions of use, defining the owner of the data elements and “WHO” will enforce the agreement
- Legislations, regulations and penalties, such as fines for breach of legislation or for inappropriate use
- Unambiguous policies and guidelines, accessible by the public
- Developing a register of approved users, and defining how they may use data. A suggestion was the use of “access control matrices”, auditing and classification

- Communicating frequently with users about their rights and responsibilities with respect to data use. Educating users is particularly important; “Educate staff in government agencies about how data can be used, and what tabs governments are keeping. E.g. internal audit systems that run on intrusion detection systems might keep logs of all transactions to do with spatial and statistical data”
- Limiting sharing between departments and agencies, particularly within the Government sector, as it is not possible to distribute data and be sure that the data will be used appropriately
- Introducing physical security on assets to ensure correct storage, and prevent illegitimate physical access of data
- Encouraging a coordinated ‘whole-of-Government’ approach to data protection
- Prohibiting companies from selling data, which is an extreme option and is not realistic given the nature of the commercial data sector
- Using “common sense”

Information and Communication Technologies (ICTs) facilitate access to public data through the Internet, and consequently are at the centre of the public data availability dilemma. However, there is the potential to supplement the above-mentioned security techniques with technical measures in certain situations, and use ICT to assist in protecting and restricting access to sensitive datasets. According to the surveyed security experts, technical security mechanisms may include:

- Secure networks not displayed to the public on networks and the Internet, containing regular and real time encryption, logging, auditing, standard protection from damage (firewalls, intrusion detection systems) and appropriate filters
- Access control, and password protection, requiring identity checks to be performed for more sensitive data, such as defence information
- Security clearance for access to sensitive data, including providing proof of identity and justification in terms of data use
- “Deliberately non-integrated systems”
- “Central storage and distributed access”
- Review and update of technical security techniques, and measuring their effectiveness

7 Conclusion

A key outcome of this survey is that the public data availability situation may be interpreted in many ways, and one solution alone (for example, a technical solution) cannot be employed. Rather, there is the need for a responsive solution that targets

specific stakeholders, and is concerned with the sensitivity of public data in terms of compromising the CIP process, and protecting individual CI elements. However, it is important to note that the response suggested requires further work, and that the approach itself is not infallible.

An important point raised by a respondent is that perhaps the public data availability dilemma is being approached from an incorrect angle, that we should not address the issue only in terms of the mechanisms that can be implemented. Rather, it may be “about facing the root problems of terrorism, and addressing them.” Extending this point beyond the terrorist threat, it may be valuable to address other adverse issues such as vandalism, fraud and competitive intelligence, and engage in why such activities take place and attempt to limit or address the causes. This requires further research, as it is beyond the scope of this paper.

When considering critical infrastructure protection, it is worth noting that CIP is one aspect of a broader solution. As stated by a security expert, “a government cannot hope to achieve a comprehensive approach to critical infrastructure protection if they are giving away data about their own infrastructure.” Providing a wealth of CI-related data online can result in unscrupulous individuals conducting their own risk assessments, defining areas where the greatest losses will occur, and easily identifying the location of the CI elements. However, censorship is not the answer.

As demonstrated in this paper, a balance is crucial and many elements such as employing a structured approach using technical and non-technical mechanisms, in addition to determining the root cause of detrimental activities that can be carried out using public data, is essential.

References

- Abbas, R. (2006). ‘The Risk of Public Data Availability on Critical Infrastructure Protection’, in K. Michael and M.G. Michael (eds), *The Social Implications of Information Security Measures on Citizens and Business*, University of Wollongong, NSW, Australia, pp. 201–212.
- ASIO (2006). ‘ASIO’s Work: Critical Infrastructure Protection’ [Online], Available: www.asio.gov.au/Work/Content/CIP.htm [Accessed January, 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].
- Chakrabarty, M. and Mendonca, D. (2004). ‘Integrating Visual and Mathematical Models for the Management of Independent Critical Infrastructures’, *IEEE International Conference on Systems, Man and Cybernetics*: 1179–1184.
- 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].

- Jones, E.V., Lyford, V.J., Qazi, M. K., Solan, N. J. and Haimes, Y.Y. (2003). Virginia's Critical Infrastructure Protection Study. *Systems and Information Engineering Design Symposium, IEEE*: 177-182.
- Luijff, 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.
- Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems Magazine, IEEE* 21(6): 11-25.
- Scholand, A. J., Linebarger, J. M. and Ehlen, M. A. (2005). Thoughts on Critical Infrastructure Collaboration. *Sandia National Laboratories, ACM* November 6-9: 344-345.
- Thuraisingham, B. (n.d.). Data Mining, National Security, Privacy and Civil Liberties. *SIGKDD Explorations* 4(2): 1-5.

11

Re-using public sector information (PSI) for profit: Who's data is it anyway?

Mark Burdon

PhD Candidate, Faculty of Law, Queensland University of Technology

Abstract

This paper will outline legal and policy developments regarding the commercial re-use of public sector information (PSI) by government agencies and the information privacy and national security concerns that may arise. Whether governments should be allowed to re-use their information for income generation purposes is a contentious issue as exemplified by the opposing philosophical rationales of the EU and the USA. Australian governments take a more pragmatic approach that has resulted in a diffusion of different policy statements. This paper will highlight real life examples of commercial re-use of PSI activities that have caused information privacy concerns in the UK and the USA along with a brief overview of Australian legislative and information policy implications. In conclusion, the paper will discuss the potential influences that governmental income generation activities may have upon national security and the societal benefits occurring from an open and transparent information society.

Keywords: commercialisation, public sector information (PSI), information privacy, e-government, information ownership and consent.

1 Introduction

The last decade has witnessed the fruition of e-government aims into practical strategies and implemented projects. The enhanced development of information and communication technologies (ICTs) in government has created new opportunities for agencies to collect, share and re-use their data. At the same time, the commercial worth of governmental data sets and value added information products/services have increased. Government agencies 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.

Underlying commercial re-use issues represent differing philosophical outlooks that place different emphases on the balance between public access rights to government information and the economic benefits that can be gained from the marketisation of government information. These philosophical differences are evident in the commercial re-use of PSI policies that have been developed in the EU and the USA. Australian governments take a more pragmatic outlook which makes it more difficult to ascertain the existence of a comprehensive philosophical intention.

The prospect of increasing revenue through the commercial re-use of PSI is clearly appealing for governments and their agencies. However, it raises a key question about the technocratic public administrations of the future, namely, what happens to e-government organisations when they move from being purely service providers to market-oriented, income generators? This change could see a re-balancing of government priorities that favour income generation policies over previously held democratic and social norms that defined the scope, nature and the boundaries of the relationship between governments and their citizens. Moreover, a paradigmatic change of governmental ethos could also impact upon the realm of national security. The enhanced publication of PSI, particularly for income generation purposes, could lead to conflicts within, and between government agencies, regarding the restriction and distribution of information.

This is not merely an academic question as the EU's PSI policies now attach economic considerations to one of the historical core functions of government – the collection, storage and use of data. These shifting priorities become more apparent when the commercial re-use of PSI is addressed against the information privacy legal obligations placed upon agencies. Ultimately, the shifting priorities, boundaries and relationships will influence the shape of and prospects for a transparent and open information society, which in turn, will influence notions of national security.

2 Re-use of public sector information

At the onset, it is important to acknowledge the unique position that governments have as a collector of public data (OECD 2006). Agencies have statutory means to enforce disclosure and they are the only feasible provider of comprehensive national

data sets (Rowlands 1995, 227). However, defining PSI is not a simple task as can first be assumed. This is due to the inherent tensions between rights of public access and governmental economic benefits from commercialisation which result in changing notions and different definitions of PSI (Blakemore and Craglia 2006, 2). During the course of the last two decades, EU policy objectives have reflected these changing notions, as PSI has been defined in different ways, at different times, to reflect different policy and economic ambitions (Aichholzer 2004).

2.1 EU – the commercialisation rationale

The first attempt to develop an EU-wide policy on PSI was the “Guidelines for Improving the Synergy between the Public and Private Sectors in the Information Market” (European Commission 1989) which sought to synergise public and private sector initiatives to stimulate economic growth in the European information market. The initial reception to the idea of commercially re-using PSI was luke warm at best. The Guidelines were criticised for not paying enough attention to the importance of public access to government information, but at the same time, the private sector was also critical because the Guidelines had no binding force on the member states (Janssen and Dumortier 2003, 187). The Guidelines were followed in the early to mid 1990’s by three European Commission reports called the “PUBLAW Reports” which sought to examine why the Guidelines failed. The reports ultimately resulted in a European Commission Green Paper entitled “Public sector information: A key resource for Europe” (1998) which was part of a consultative process involving the public and private sectors, citizens and user groups to rekindle the ailing prospects of an EU-wide internal information market.

The Green Paper initiated an European Commission communication in 2001 which lay the foundations for a commercial re-use of PSI directive (European Commission 2001). The economic importance regarding the commercial re-use (or exploitation as referred to by the Communication) of PSI was confirmed as the clear and unambiguous priority of the Commission (Janssen and Dumortier 2003, 194). As such, the Communication laid the foundation for a governance framework that would alleviate those problems encountered during the previous decade, such as different national administrative rules, digital formats and pricing regimes. Its broad economic intent lead to the provision of a general principle of commercial re-use, namely “whenever public sector information is generally accessible, commercial re-use should be considered” (Janssen and Dumortier 2003, 195).

The Communication became a Commission proposal (European Commission 2002) which eventually resulted in a commercial re-use EU-wide directive the following year (European Commission 2003). Finally, fourteen years after the publication of the 1989 Synergy Guidelines, a confirmed EU-wide commercial re-use of PSI policy was implemented. The Commission had consistently stated that one of its aims was to harmonise member state commercial re-use of PSI rules. Yet despite that, the Directive left any commercial re-use decision to the discretion of

member state governments. Thus making it very difficult to develop one unified, EU-wide PSI framework (Pas and Du Vuyst 2004, 12). The Directive is also solely concerned with the public sector and no conditions were placed upon private sector information brokers. Again, this reflects the Commission's commitment to realizing the economic potential of PSI despite the negative consequences that may arise from placing no restrictions on the private sector (Pas and Du Vuyst 2004, 12).

Paradoxically, and rather ambiguously, the Directive does create income generation opportunities for government agencies by allowing public sector bodies to make profits from the commercial re-use of their PSI (European Commission 2003, Art. 14). Government agencies can seek to recover costs as long as any charge is a "reasonable return on investment" and is not "excessive". This would appear to vary somewhere in between a marginal cost recovery and market cost return which provides public sector agencies with income generation opportunities (Pas and Du Vuyst 2004, 4). The UK is one member state that has embraced the commercial purposes of the Directive and has created the Office of Public Sector Information (OPSI) to enhance commercial opportunities and to rationalise the development of information policy across the public sector (Office of Public Sector Information 2007). The OPSI regulates PSI transactions involving government agencies and also investigates complaints against agencies made under the Re-use of Public Sector Information Regulations issued in 2005.

Not surprisingly, given its contradictory nature, the Directive has come under some criticism. Blakemore and Craglia (2006, 3) state that the Directive is "based on an untested assumption that there is a latent demand for information that is unfulfilled because of technological and policy 'barriers' that therefore need to be removed". As such, the commercial re-use of PSI is a market oriented approach that has a rationalistic and a linear viewpoint that overly focuses on technologies, information and benefits but does not encapsulate the true complexities of the situation. Several authors have also criticized the overt economic interests of the EU's policies which overshadow the information access rights of citizens (Aichholzer 2004, Pas 2002, Pas and Du Vuyst 2004, Prins 2004).

2.2 USA – the principle of free and open access

At a Federal level, the situation in the USA is somewhat different. Unlike the EU, the dichotomy between the commercial re-use of PSI and the information access rights of citizens does not exist. Instead, the Federal Government is not allowed to differentiate between general access and commercial re-use (Papapavlou 1999, 3). The vast majority of Federal Government information is therefore freely available to the private sector and the public. The purpose of this approach is to ensure that taxpayers do not pay twice for government information and to encourage the widest possible dissemination of information (Pas 2002).

Four existing laws form the PSI foundation of the US Federal Government (Gellman 2004, 123). The first is the First Amendment of the US Constitution

which guarantees freedom of speech and promotes open political dialogue. Whilst the First Amendment does not specifically preclude the Federal Government from commercially re-using PSI, it sets a tone of prohibiting government interference in the marketplace that has been followed by subsequent pieces of legislation (Gellman 1996). For example, rule 34 of the Copyright Act 1976 expressly states copyright protection is not available for any work to the US Government. The effect of the legislation is to place all Federal Government information in the public domain (Gellman 1996). The public interest is therefore “served by keeping governmentally created works as free as possible of potential restrictions on dissemination” (Gellman 2004, 126). The practical effect is that anyone can reproduce and re-use government information and sell it at any price. However, the prohibition of copyright does not extend to state governments who are allowed to copyright their data and therefore have the legal sanction to commercially re-use their information.

The third piece of legislation, the Freedom of Information Act 1966, ensures public access to government information. The act permits any person to request any record in the possession of a federal agency in order to establish a culture of disclosure for government records (Gellman 2004, 124). In 1996, amendments were made to act to reflect technological changes and the advent of electronic recordkeeping. Accordingly, if an agency receives three or more requests for the same records, the agency should make the records available on its website thus adding a wider information dissemination purpose to the public access aims of the legislation (Gellman 2004, 125). The final piece of legislation, the Paperwork Reduction Act 1995 aims to prevent bureaucratic control of information by directing agencies to ensure that information is disseminated to the public in a timely and equitable manner. A key purpose of the legislation is to ensure that government does not have a monopoly over its information and thus prevents an agency from commercially re-using its own PSI (Gellman 2004, 130).

2.3 Australia – the pragmatic approach

The Australian situation, at the Federal level, is philosophically less clear cut as there appears to be no coherent or overriding PSI policy agenda. Instead, there is a mix of different policy objectives relating to intellectual property principles, the development of the information economy and cost recovery guidelines. For example, the “Intellectual Property Principles for Australian Government Agencies” (Australian Government Attorney-General’s Department 2005) provides “a broad policy framework for intellectual property management” that covers a wide range of works produced by the Commonwealth. Despite this, agencies are nonetheless encouraged to develop their own individual intellectual property management frameworks that reflect their own needs and objectives. Whilst the principles provide an overarching guideline for Commonwealth agencies, the ultimate form of implementation is left to the agencies themselves.

Principles 11 to 15 are particularly relevant to the issue of commercialising

PSI. Principle 11 states that agencies “should encourage public use and easy access to copyright material” that is primary to the function of government. This is similar to the access rights provisions of both the EU and the USA which deem fundamental government information should be made freely available. However, the use of the words “should encourage” is by no means as strong as the obligations that US Federal Government agencies must comply with. Principle 13 states that Commonwealth agencies should be responsive to opportunities for commercial use and exploitation of intellectual property. Furthermore, agencies should consider the potential benefits that may be realised through commercialisation by the private sector to create cost savings and continued product development. Principle 13 therefore supports Commonwealth agencies to undertake commercialisation of PSI activities particularly in conjunction with the private sector.

The Intellectual Property Principles recognise the importance of making core government information freely available (like the USA and the EU) and offer a watered down version of the EU’s marketisation strategy. That said, the importance of re-using PSI in the development of the information economy is highlighted as a priority in “Australia’s Strategic Framework for the Information Economy 2004-06” (Australian Government Department of Communications 2004). Strategy 4.3 of the Approach recognises the necessity for a structured approach to the collection and re-use of information by Australian governments with the private sector (2004, 54). The Approach confirms that tensions may arise between whole-of government and single agency initiatives but it is silent on the issue of agency PSI commercialisation activities, especially as a foundation for information market development. In that regard, the Approach is different to the PSI policies adopted by the EU.

Furthermore, the “Australian Government Cost Recovery Guidelines” (Australian Government Department of Finance and Administration 2005) provide a framework to assist agencies to design and implement cost recovery arrangements. The Guideline’s overarching aim is to ensure that coherent cost recovery practices, regarding fees for goods and services, are implemented uniformly. As such, the Guidelines are seen as an “important means of improving the efficiency with which Australian Government products and services are produced and consumed” (2005, 11). Finally, one other guideline worth noting is the “Commonwealth IT IP Guidelines” (Australian Government Department of Communications 2004) which provides a guide for agencies to maximise the benefits from Commonwealth IT related intellectual property. However, whilst recognising the benefits that can be gained out of commercialisation, the IT Guidelines do not cover government information *per se*, but instead, cover elements such as documentation, databases, websites, methodologies and models.

2.4 Summary

The different philosophies of the EU and the US reflect differing priorities regarding the role of PSI and governmental information dissemination. The EU

prioritises economic purposes and views PSI as a commodity that can be used to develop an EU-wide information market. The primary relationship of concern in the EU is between government and the private sector. Citizen rights of access are secondary. The US prioritises access rights over economic concerns and the primary purpose of PSI laws and policies is to ensure that government information, at least at the Federal level, is made as freely and widely available as possible. The primary relationship of concern is between government and the access rights of individuals which also includes the private sector. In Australia, Commonwealth policy on the commercial re-use of PSI is somewhat fractured. When viewed as a whole, commercial re-use of PSI policies show the absence of a dominant philosophical outlook, whether it be economic or access oriented, and instead places commercial re-use policy decisions in the hands of individual agencies, who are compelled to operate within the bounds of different guidelines.

3 Information privacy concerns

Information privacy laws and regulations consign upon data collectors various constraints that govern the collection, the use and the dissemination of personal information. Information privacy therefore ensures that information about an individual is kept confidential and is only used for certain purposes, which that person, has consented to (Bannister 2005). Within the context of e-government, an analysis of information privacy issues is integral to resolve the trust tensions that arise from the enhanced use of technologies by governments and the anxieties of citizens regarding the use that their information is put to (Dutton, et al. 2005, 13). Those same tensions are more likely to arise with the commercial re-use of PSI because personal data could possibly be used in a way beyond the original purpose for which it was collected and for the purposes of governmental income generation. This may ultimately result in citizens having even less control and influence over the handling of their data by government agencies.

3.1 Privacy Act implications – Information Privacy Principle (IPP) 10

Unlike the situation regarding commercial re-use of PSI policies, there is largely one overarching Australian information privacy law that governs the information collection, storage and use activities of the different levels of government and the private sector. *The Privacy Act 1988 (Cth)* governs the activities of Commonwealth and ACT government agencies and forms the basis of separate state-based legislation that regulates state government agencies (Paterson 2005, 79).

Section 6(1) of the Act defines personal information as information or an opinion that can identify a person. This definition has a broad application and a record does not have to identify a person directly for it to be classed as personal information. For example, it is possible for a record to be classed as personal information, even if a person is not mentioned by name, but he/she can be identified by cross-referencing with data in the record, with other data that uniquely identifies that individual.

For the purposes of the Act, 'record' is also broadly defined to include a document, a database or a photograph of other pictorial representation of a person (Paterson 2005, 61). Section 13(a) indicates that agency practices can constitute "an actionable interference" with an individual's privacy if that practice or act breaches one of the IPPs. Under section 36, an individual has recourse for action under a breach of the Act by notifying the Privacy Commissioner of their grievance. Section 46 provides the Commissioner with investigatory powers and the Commissioner can direct relevant parties to attend a conference regarding any complaints. Following investigation of a complaint, the Commissioner has a number of powers under section 52(1)(b), including the power to make a declaration that the awarding compensation for any damage suffered by a breach of privacy. To enforce or appeal determinations by the Commissioner under section 55A, an action must be initiated in the Federal Court or the Federal Magistrates Court.

An actionable interference will be assessed by reference to the IPPs as detailed in section 14. For the purposes of this paper, IPP 10 is of particular importance because it limits the use of personal information by governmental organisations. It states that an agency must only use personal information for the purpose for which it was originally obtained unless:

- a. An individual has consented to the use of their information for another purpose;
- b. The agency reasonably believes that use of the information is beyond the scope for which it was originally collected and is necessary to prevent or lessen a serious and imminent threat to life or the health of a person;
- c. The agency is authorised by law to use the information for a different purpose;
- d. The agency is using the information for another purpose that is reasonably necessary for the enforcement of criminal law, or laws relating to pecuniary penalties for the protection of public revenue; or
- e. The agency is using the information in a way that is directly related to the purpose for which it is collected.

A difficulty arises for government agencies regarding the commercial re-use of PSI because of the principle of consent that is fundamental to IPP 10. In practice, a government agency is likely to be mandated by a certain piece of legislation to collect data, including personal data from individuals. Those individuals consent to providing their data for the original purpose it is collected. This 'primary purpose' of data collection fulfils the agency's legislative obligations and fulfils an essential administrative function of the agency. However, when an agency attempts to commercially re-use its information, either as raw data or as value added information/product, it does so for a 'secondary commercial purpose'. In this situation, it is possible that an individual has consented to the primary purpose but may not have

consented to the secondary commercial purpose.

The issue at hand is therefore whether government agencies actually have the legal means under the IPPs, and IPP 10 in particular, to collect and to re-use personally related information for income generation purposes. The key concern is whether agencies can legitimately claim a 'secondary commercial use' for personally related information under one of the exemptions of IPP 10 listed above. Otherwise the consent of those individuals whose data is being re-used may be required. If that is the case, given the size of some government data sets, seeking the consent of individuals could prove to be administratively difficult and perhaps economically infeasible. Moreover, given the economic pressures now being placed on government agencies to generate their own income, there could potentially be an economic incentive to bypass information privacy legal obligations. Especially in situations that are perceived as 'harmless' and involve tangential or indirect personal information that requires some form of re-identification in order to identify individual persons. Two actual examples of PSI re-use problems from the USA and the UK highlight such situations of concern where an individual's control over his/her personal information can be seen to have been eroded by the economic priorities of agencies.

3.2 US and UK situations of concern – Kehoe and the DVLA

In the US case of *Kehoe v Fidelity Federal Bank & Trust*, (4 S.Ct. 1612 (Mem.), 21 F.3d 1209 126), a class action, involving hundreds of thousands of persons, was brought against the Fidelity Bank regarding its purchase of 565,600 names and addresses of Florida citizens from the Florida State Government's Department of Motor Vehicles (DMV). Upon purchase, the Bank used the DMV's information to mass mail Florida residents', in three counties, about car loan advertisements. This was in direct contravention of the Federal Drivers Privacy Protection Act (18 U.S.C. § 2721) (DPPA) which requires state governments to protect the privacy of an individual's personal information contained in motor vehicle records (Electronic Privacy Information Center 2005).

The DPPA was enacted in 1993 to deter would be stalkers, and their ilk, from gaining access to existing or potential victims via publicly listed motor vehicle records. A further amendment was put forward in 1999 that required a state DMV to obtain the consent of any individual whose driver license information was being released, including commercial re-use for bulk marketing purposes. In the *Kehoe* case, the plaintiffs' consent was required before the DMV could re-use and sell their information to the Bank. However, the 1999 amendment, which was enacted in 2000 by the Florida legislature, was never updated into Florida law because of an oversight. As such, driver licence information continued to be used for commercial purposes and without consent. The US District Court for the Southern District of Florida found for the Bank at first instance because the plaintiffs' could not demonstrate that the Bank's breach of the DPPA did not cause them actual harm. The plaintiffs' appealed to the 11th Circuit Court of Appeals and the court overturned the decision

holding that it was not a requirement under the DPPA to prove actual harm for a claim of damages. The Bank was required to pay \$US50 million to the plaintiffs' for using their personal information for marketing purposes without their consent.

In 2005, the UK Government's Driver and Vehicle Licensing Agency (DVLA) also encountered problems with selling driver licence information. The DVLA is responsible for collecting data on persons who have been issued with a UK driving license and for vehicles registered within the UK. For a small sum, the DVLA routinely sold its driver licence information to certain companies, such as car park managers, car clamping firms etc. For an extra charge of around £3,000, the DVLA authorised direct access to its database system which allowed companies to type in a registration number and to download corresponding personal information about the registered car owner (Purves 2005). The DVLA claimed that it was obliged to commercially re-use its PSI because of a 2002 statutory instrument that required the organisation to sell information to anyone with 'a reasonable cause' (Purves 2005).

Despite the fact that only companies with a reasonable cause were supposed to access the DVLA's database, the agency authorised access to one of Europe's largest credit card companies, who are were known to employ extensive direct mailing tactics, on the pretence that the company had a reasonable cause because it owned a private car park at its central office (Delgado, et al. 2005). More worryingly, the DVLA also sold its information to a private car clamping firm whose directors were found guilty of blackmailing unsuspecting motorists. The blackmailers sent threatening letters to victims citing their registration details and claiming that a spurious parking violation had taken place (Purves 2005). Subsequent critical media coverage about the DVLA's commercial activities, led to the Department of Transport, which houses the DVLA under its accountability framework, to respond by establishing a public review and consultation exercise (McCue 2006). The review resulted in 14 new measures including detailed guidance on what constitutes a reasonable cause; a requirement for organisations to be members of an accredited trade association and the instigation of a new complaints procedure.

3.3 Discussion

Several points of interest arise from the *Kehoe* and the DVLA examples. Firstly, the construction of the DPPA is unusual in the context of information privacy and data protection laws. The DPPA was established to deter would be stalkers and it therefore obliges the buyers, rather than the collectors (or sellers) of data, to act within certain confines. As such, in *Kehoe*, an action was brought against the Bank but no action was brought against the Florida DMV. Contrast that with the DVLA example, where the agency received voluble criticism that resulted in a consultation review of its actions and the implementation of stricter guidelines to correct its information re-selling practices.

At face value, whilst acknowledging the different circumstances, this maybe a

reflection of how the different PSI philosophies of the US and the UK impact upon information privacy concerns. In the US, the general perception is that government information should be freely available. Hence the focus placed on the actions of the information buyer rather than the provider. The UK, on the other hand, has accepted the income generation activities of governmental agencies with a consequence that the commercial re-use of PSI may come with a price tag. Hence the criticism directed at the DVLA as a seller of information rather than the companies who illegitimately used that information. In particular, it is interesting to note that none of the press articles overtly criticised the credit card company for using the DVLA data for mass mailings when it was clearly using personal information for a purpose beyond the reasonable cause requirement.

This leads to the key point of interest regarding the consent of individuals for a secondary commercial purpose. Both examples provide different methods of obtaining consent but both failed to supply an effective means of privacy protection regarding the commercial re-use of PSI. For example, section 2721 of the DPPA indicates the purposes for which motor vehicle records can be used. This includes a provision for mass mailing solicitations if the information provider has obtained the express consent from the individuals named in the mailing list. If an individual has not provided consent to the release of his/her motor vehicle record for the purpose of mass mailings then the DPPA prohibits the use of their data in that specific way (Electronic Privacy Information Center 2005). In the *Kehoe* case, the consent requirement was inadvertently not enacted and the DMV continued to sell its information without restriction. However, the actions of the Florida DMV are still open to question given that they forwarded personal information directly to a third-party mass mailing service retained by the Bank. The mass mailing service then mailed the Bank's advertisements to individuals. Bearing in mind the comments above regarding the open access model to PSI in the US, it is remarkable that the Florida DMV forwarded their information straight to a direct mailing firm, thus surely knowing the purpose that the Bank was going to use the information for. Regardless of whether the consent requirement was enacted or not, it would certainly appear that the information privacy of Florida residents was not their primary concern.

In the DVLA example, only interested parties (i.e. those with a reasonable cause) should have been able to gain access to driver's personal information. However, as detailed above, the practical definition of 'a reasonable cause' was so broad that it allowed illegitimate access by companies, and once information was accessed, there was practically no restriction on the use that the information was put to. The implicit assumption behind the DVLA's commercial actions was that individual drivers had consented to any re-use of their information. This was clearly not the case as witnessed by the widespread criticism heaped on the DVLA after the media broke the story. As such, both cases represent a failure of government agencies to obtain individual consent for a 'secondary commercial purpose' which highlights

either (a) a disturbing lack of concern regarding information privacy issues entailing a cavalier attitude to the sale of personal information or (b) an elevated income generation focus, particularly in the DVLA's case, which places commercialisation needs over information privacy obligations.

4 National security implications

The *Kehoe* and DVLA examples underline information privacy concerns arising from the commercialisation of PSI that have an effect at an individual level. It is further possible to define issues that give rise to national security concerns arising from the commercialisation of PSI which take place at a governmental level.

Firstly, it is worth noting just how cheaply personal information was being sold for in both cases. In *Kehoe*, the Bank paid \$US5,656 for the personal information of more than half a million Florida residents which approximates to only one cent for each name and address they bought. The DVLA sold details of individuals for only £2.50 per record. Nevertheless, the DVLA earned £6.3 million in 2005 from its commercial re-use of personal information (McCue 2006) which gives a clear indication of just how many records were routinely being re-used and sold. Furthermore, evidence from the US has also suggested that state based DMV's have been susceptible to fraud, corruption and weak security practices (Center for Democracy and Technology 2005). For example, in December 2003 a former state employee from the Nevada DMV pleaded guilty to receiving bribes totalling more than \$US300,000 to provide unauthorised identification documents to illegal immigrants. In June 2002, 36 people, including DMV staff, were indicted in a complex criminal operation that involved the fraudulent issue of New Jersey driving licences. The criminals involved were so sophisticated, and the demand so great, that different brokers competed against each other to provide the best choice of illegal services at a price to suit (Office of the New Jersey Attorney General 2002).

This shows the commercial value of driving licence personal information. In the case of the 'legitimate' sales of the Florida DMV and the DVLA, the commercial value exists because of the potential uses that third parties can utilise the information for (e.g. direct marketing). In the case of fraudulent or other criminal acts, a commercial value exists for the provision of falsely accredited identification that can be used to dishonestly confirm a false identity. Although the reasons behind the agency sales and the criminal acts are very different, they nonetheless provide consequential threats for national security because both situations provide greater access to the fundamental material of identity theft – personal information that can, with relative ease, be recycled into a fraudulent identity. In fact, it is astonishing, at a time when identity theft is fast becoming the highest crime concern in most first world countries, that both agencies were selling personal information at basement store prices, and more worryingly, paid scant regard to who they were providing it to. So much so, that is difficult to avoid the conclusion that commercial reasons,

whether directly or indirectly, outweighed the potential threats of national security arising from the misuse of personal information for identity theft reasons.

Issues regarding the governmental commercialisation of personal information, particularly driving licence data, may therefore impact upon national security concerns. Whilst governments have recognised the security issues arising from the identification purposes of driving licences, they have not been as quick to recognise the concerns that may arise through the commercialisation of driving licence information. As such, legislative and technical responses have tended to focus on the construction of more robust forms of licence that can be used for identification purposes, as exemplified by the Real ID Act in the USA and the Queensland Smart Driving Licence. However, the personal data that form those licences has, and is continuing, to be sold to commercial entities and other bodies.

This creates a somewhat paradoxical situation. Governments throughout the world are setting aside large amounts of financial, legislative and technical resources to create stronger forms of driving licence identification. Yet the information behind those licences is commercially available at inexpensive prices with little recourse as to who is buying it. As highlighted above, the DVLA received just criticism regarding its commercial practices that infringed individual privacy and which provided foundational support for criminal fraudsters. Those same criticisms are equally applicable to national security concerns.

It should also be recognised that governmental commercial information transactions with legitimate sources (e.g. information brokers), still give rise to national security issues, due to the reduction of control that government agencies have over information once it has been sold to a commercial third party. Whilst a government agency can licence certain uses that its information should and should not be put to, the ultimate decision on who a commercial third party sells information to resides with the third party. It is difficult to imagine that any commercial third party could have done as poor a job as the DVLA but it has to be acknowledged that there are potentially less stringent checks and requirements imposed on the private sector information broker in comparison to the public sector, government agency. In effect, once governmental information is distributed for sale, it is difficult for governments to control who it is ultimately sold to and the uses that the information is put to. That said, it is clearly unacceptable for a government agency to provide, let alone sell, personal information to an illegal or illegitimate source.

Thus far, this paper has focused on the information privacy and national security issues that arise from driving licence personal information. More complex privacy and national security issues may arise from the commercialisation of geospatial information because information is derived from multiple agency data sources, it is replete in a number of different data formats and it can be interpreted in multiple ways and beyond the purpose it was originally intended for (Onsrud 2003, Onsrud, et al. 1994, Snellen 2000, ANZLIC 2004). It is not within the scope of this paper to cover the issue in depth but it is important to highlight in the context of national

security concerns arising from the commercialisation of geospatial PSI. The enhanced proliferation and publication of governmental geospatial information may have the consequence of putting information in the public domain that may more easily be available to fall into the proverbial 'wrong hands'. However, whilst it is important to recognise this point, it is equally important to balance risks arising from extended publication with the public good emanating from wider distribution of governmental information (Onsrud 2003).

5 Conclusion

This paper has highlighted the different philosophical approaches of the EU, the USA and the Australian Federal Government regarding the commercial re-use of PSI. The EU's outlook is overtly economic and encourages member governments to commercially re-use PSI for the development of an EU-wide information economy. The USA adopts a different perspective, at least at the Federal level, which aims to make government information freely available. The Australian Federal Government lies somewhere in the middle of the scale and adopts a pragmatic approach that is not as philosophically guided as either the EU or the USA. The paper continued to highlight information privacy concerns for governments regarding consent issues. In Australia, IPP 10 is of particular issue and actual US and UK examples highlighted situations where such consent concerns have arisen.

The *Kehoe* and *DVLA* examples highlight the sheer volume of PSI that is commercially re-used for governmental income generation purposes. This in itself raises implications for the prospect of an open, transparent and secure information society. A balancing of societal interests is required which reflects the differing priorities within governments and their effects on individuals. On one side of the scale, we have the societal interest arising from access to government information whether it is in the form of free and open access, to enhance democracy, or whether it is in the form of the commercial re-use of PSI, to enhance the information economy. On the other side, we have the societal interest arising from the trust relationship between citizens and their governments which is founded upon and constructed around the keystone notion of information privacy. At face value, the two sides of the interest scale appear to be, if not irreconcilable, then certainly at conflict with each other. Both interests represent competing values involving the requirements of economically self-sufficient governments to sell, restrict and distribute their information versus the individual citizen's right to access and to control the use and re-use of their personal information. The complex reconciliation of these interests is further compounded when issues of national security are added to this mix.

It is perhaps easier to identify the conflicting societal interests entailed in the commercial re-use of PSI and the information privacy of citizens than it is to counterbalance fundamental competing concerns, especially in light of national security issues. It is perhaps equally clear that a balance will not be found by simply examining and updating PSI, information privacy and national security legislation.

Current laws do not adequately reflect the conceptual complexity and the democratic importance of maintaining a balance between governmental income generation, through the commercial re-use of PSI; the information privacy of citizens and the national security requirements of governments.

All of which points to the fact that government agencies need to pay care and attention to privacy and national security issues when making decisions to commercialise PSI held under their custodianship. Both the *Kehoe* and the DVLA examples highlight concerns that can arise from the commercialisation of PSI and the negative consequences that can emerge for government agencies that have an overt income generation outlook. The advent of wide spread, identity related crimes and increased terrorist threats place greater requirements on government agencies to think carefully before they adopt new PSI commercialisation strategies or they re-engage in existing commercial transactions. Otherwise advanced and unchecked marketisation of government information could have a detrimental effect on both individual privacy and societal national security.

6 References

- Aichholzer, G. (2004) "Electronic Access to Public Sector Information: Some Key Issues." In *Electronic Government*, 525-28: SpringerLink.
- Australian Government Attorney-General's Department (2005) "Intellectual Property Principles for Australian Government Agencies." Available at [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(22D92C3251275720C801B3314F7A9BA2\)~Statement+of+IP+Principles+for+Australian+Government+Agencies-t.pdf/\\$file/Statement+of+IP+Principles+for+Australian+Government+Agencies-t.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(22D92C3251275720C801B3314F7A9BA2)~Statement+of+IP+Principles+for+Australian+Government+Agencies-t.pdf/$file/Statement+of+IP+Principles+for+Australian+Government+Agencies-t.pdf) (Accessed 7 June 2007)
- Australian Government Department of Communications, Information Technology and the Arts (2004) "Australia's Strategic Framework for the Information Economy 2004-2006: 'Opportunities and Challenges for the Information Age'." Available at http://www.dcita.gov.au/__data/assets/pdf_file/20457/New_SFIE_July_2004_final.pdf (Accessed 1 June 2007)
- Australian Government Department of Communications, Information Technology and the Arts (2004) "Management and Commercialisation of Commonwealth Intellectual Property in the Field of Information Technology." Available at http://archive.dcita.gov.au/__data/assets/pdf_file/10079/Commonwealth_IT_IP_Guidelines.pdf (Accessed 1 June 2007)
- Australian Government Department of Finance and Administration (2005) "Australian Government Cost Recovery Guidelines." Available at http://www.finance.gov.au/finframework/docs/Cost_Recovery_Guidelines.pdf (Accessed 1 June 2007)
- Bannister, F. (2005) "The Panoptic State: Privacy, Surveillance and the Balance of Risk." *Information Polity: The International Journal of Government & Democracy in the Information Age* 10: 65-78.

- Blakemore, M., and Craglia, M. (2006) "Access to Public-Sector Information in Europe: Policy, Rights, and Obligations." *Information Society* 22: 13-24.
- Center for Democracy and Technology. (2005) "Tracking Security at State Motor Vehicle Offices." Available at <http://www.cdt.org/privacy/030131motorvehicle.shtml>. (Accessed 18 September 2007)
- Delgado, M., Ludgate, R. and Nichol, M. (2005) "DVLA Sells Your Details to Criminals." *Mail on Sunday*, 27 November.
- Dutton, W., et al. (2005) "The Cyber Trust Tension in E-Government: Balancing Identity, Privacy, Security." *Information Polity: The International Journal of Government & Democracy in the Information Age* 10: 13-23.
- Electronic Privacy Information Center. "The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record." Available at <http://www.epic.org/privacy/drivers/>. (Accessed 27 July 2007)
- European Commission (2003) "Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Reuse of Public Sector Information". Available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_345/l_34520031231en00900096.pdf (Accessed 30 April)
- European Commission (2001) "eEurope 2002: Creating a EU Framework for the Exploitation of Public Sector Information." Available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/eeurope/2001_607_en.pdf (Accessed at 11 May 2007)
- European Commission (1989) "Guidelines for Improving the Synergy between the Public and Private Sectors in the Information Market." Available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/brochure/1989_public_sector_guidelines_en.pdf (Accessed 8 May 2007)
- European Commission (2002) "Proposal for a Directive of the European Parliament and of the Council on the Re-Use and Commercial Exploitation of Public Sector Documents." Available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/en.pdf (Accessed 11 May 2007)
- European Commission (1998) "Public Sector Information: A Key Resource for Europe." Available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/green_paper/gp_en.pdf (Accessed 11 May 2007)
- Gellman, R. (1996) "The American Model of Access to and Dissemination of Public Information." In *Access To Public Information: A Key To Commercial Growth And Electronic Democracy*. Stockholm. Available at <http://europa.eu.int/ISPO/legal/stockholm/en/gellman.html> (Accessed 10 May 2007)
- Gellman, R. (2004) "The Foundations of United States Government Information Dissemination Policy." In *Public Sector Information in the Digital Age : Between Markets, Public Management and Citizens' Rights*, edited by Aichholzer, G. and Burkert, H. 123-36. Cheltenham, UK: Edward Elgar.
- Janssen, K., and Dumortier, J. (2003) "Towards a European Framework for

- the Re-Use of Public Sector Information: A Long and Winding Road.” *International Journal of Law and Information Technology* 11: 184.
- McCue, A. (2006) “DVLA Nets £6m from Sale of Motorist Details.” Available at <http://www.silicon.com/publicsector/0,3800010403,39159537,00.htm>. (Accessed 10 July 2007)
- McCue, A. (2006) “Government Considers DVLA Data Sale Restrictions.” Available at <http://www.silicon.com/publicsector/0,3800010403,39159622,00.htm>. (Accessed 10 July 2007)
- OECD (2006) “OECD Workshop on Public Sector Information: Summary.” 1-38: OECD. Available at http://www.epsipus.net/epsipus/media/files/37865140__1 (Accessed 8 July 2007)
- Office of Public Sector Information (2007). Available at <http://www.opsi.gov.uk/about/index.htm>. (Accessed 30 April 2007)
- Office of the New Jersey Attorney General. (2002) “Multi-Agency Investigation Targeted ‘Brokers’ & Corrupt DMV Employees.” Available at <http://www.state.nj.us/lps/dcj/releases/2002/dmv0624.htm> (Accessed 18 September 2007)
- Onsrud, H J. (2003) “Access to Geographic Information: Openness Versus Security.” In *Geographic Dimensions of Terrorism*, edited by S Cutter, D Richardson and T Wilbanks, 207-13: Routledge.
- Onsrud, H J, J Johnson, and X Lopez. (1994) “Protecting Personal Privacy in Using Geographic Information Systems.” *Photogrammetric Engineering and Remote Sensing*, 60:9:1083-95.
- Papapavlou, G. (1999) “Public Sector Information Initiatives in the European Union.” Available at http://webworld.unesco.org/infoethics2000/documents/paper_papapavlou.rtf. (Accessed 10/05/07)
- Pas, J. “The Commercialization of Government Information and the Proposal for a Directive Com(2002) 207 by the European Commission.” *E Law* 9, no. 4 (2002). Available at http://www.murdoch.edu.au/elaw/indices/title/pas94_abstract.html (Accessed 8 May 2007)
- Pas, J. and Du Vuyst, B. (2004) “Re-Establishing the Balance between the Public and the Private Sector: Regulating Public Sector Information Commercialization in Europe.” *Journal of Information, Law and Technology*, no. 2. Available at http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/pasanddevuyst/ (Accessed 10 May 2007)
- Paterson, M. (2005) *Freedom of Information and Privacy in Australia : Government and Information Access in the Modern State*. Chatswood: LexisNexis Butterworths.
- Prins, C. (2004) “Access to Public Sector Information: In Need of Constitutional Recognition?” In *Public Sector Information in the Digital Age : Between Markets, Public Management and Citizens’ Rights*, edited by Aichholzer, G. and Burkert, H. 48-68. Cheltenham, UK: Edward Elgar.
- Purves, L. (2005) “Licensed to Sell Your Identity.” *The Times* Available at

http://www.timesonline.co.uk/tol/comment/columnists/libby_purves/article597642.ece. (Accessed at 10 July 2007)

- Rowlands, I. (1995) "Toward Public-Private Synergy in the European Information Services Market." *Journal of Government Information* 22: 227-35.
- Snellen, Ignace Th.M. (2000) "Territorialising Governance and the State: Policy Dimensions of Geographic Information Systems." *Information Infrastructure & Policy* 6: 3: 131.

12

The Internet as a communication medium and a social space: a social constructivist approach to the use of open data

Lucy Resnyansky

Research Scientist, Defence Science and Technology Organisation

Abstract

This paper adopts a social constructivist approach in order to address issues related to the use of the Internet as a source of data. The paper identifies and critically analyses theoretical assumptions and discourses that are shaping public debates about the social impact of security practices and intelligence for an information age. These discourses promote a technological concept of the Internet as a communication medium and a powerful yet neutral technology of information storage and access. Such a construct entails assumptions and epistemologies whose usefulness has to be problematised due to the specific nature of contemporary threats and security needs. An uncritical adoption of such a construct of the Internet may have a negative impact both upon specific practices (e.g., data collection and analysis) and long-term strategies and goals. This paper outlines a concept of the Internet as a social space (a locus of social interaction) and suggests how this concept can enhance data analysis. It is argued that the use of Internet sources needs to be supported by an analysis of the conditions of their production, distribution, and consumption, and that information technologies (search engines, databases, websites, etc) need to be approached as social (discursive) practices. Such tools should provide conceptual frameworks and analytical means enabling security/intelligence practitioners to critically reflect upon data as being shaped by particular discourses, knowledge systems, and cultural worldviews. This can be achieved if social sciences were integrated in the development of technological tools supporting security/intelligence practices.

Keywords: Internet, data, social space, social constructivist approach

Today, various technologies create the means for governments, intelligence services, and even individuals to gather and interpret information about others that was historically held only in the coffers of intelligence services in Washington and Moscow. Because of this information and communications revolution, access to this information is often exceptionally fast and relatively inexpensive. The era of transparency is upon us.

At the same time, the world of terrorist cells and the illicit trade in, among other items, weapons of mass destruction that intelligence targets remains murky. Accordingly, transparency does not mean that everything is completely open, not that it should be. It means rather that there are increasingly unprecedented types and amounts of information available to any one interested party about almost any other (O'Connell 2005, p. 142).

1 Introduction

The era of transparency creates new challenges for security and intelligence and, as O'Connell (2005) notes, “[w]hile some might believe that intelligence is immune to such developments, it is actually in many ways driven by transparency” (p. 143). For security/intelligence practices aiming at an analysis of events and trends related to political violence, social conflicts, and cultural changes, transparency means that such an analysis can draw upon diverse sources of data, both classified and unclassified – from the research literature to media, computerised databases, websites created by organisations and individuals, and so on (Pillar 2004). The Internet, in particular, is widely used as a starting point, a primary resource and a powerful technology of information access (see, e.g., Reid et al. 2004).

Debates about ICTs, security and intelligence are still largely shaped by the discourses that construct technology as a powerful yet neutral augmenting tool. This construct entails and re-enforces a positivist concept of data, a cognitive concept of reliability of information sources, and a trend to ignore the diverse nature of the information/knowledge field. This, in turn, may result in sharpening the division between such activities as collection and analysis of data, which makes the interaction between security/intelligence organisations less efficient. Such a division can also be counter-productive from the perspective of the long-term security goals and the balance between security and citizen rights.

This paper's objective is to contribute to the integration of social sciences in the area of the development of tools supporting intelligence analysis and modelling (see also Resnyansky 2006; 2007a; 2007b). Integration of social scientific knowledge in the development of models and modelling (analytical) tools requires: (a) analysis of the heuristic significance of a particular social scientific theory, concept or approach; (b) critical reflection upon the sociocultural implications of the conceptual

and computational models; and (c) understanding how security practices can be affected due to the implementation of particular technological tools. In this paper, this approach is used in order to understand how the use of information sources and technologies in security/intelligence can be informed by social knowledge developed in postmodernist, critical, and social constructivist theories and approaches in sociology, communication and media studies, philosophy of technology, and sociology of science. A comprehensive outline of the relevant social scientific concepts and theories is beyond the scope of this paper. Rather, this paper aims to give a general idea of the kind of alternative knowledge that can usefully inform the development of tools supporting the use of the Internet as a source of information for intelligence analysts aiming to understand (rather than collect) data.

2 Overview

The paper starts with a critical analysis of current discourses on security, transparency and intelligence. On the one hand, I draw upon selected studies of some major challenges faced by intelligence in the age of information, such as works of O'Connell (2005) and Treverton (2003). In my opinion, these studies provide excellent overviews of the ICT-generated advantages and problems, as well as possible solutions. They also give very useful insights into the world of intelligence. My reading of these works resulted in a better understanding of a need for social scientific knowledge to be integrated in the technologies supporting intelligence analysis and data collection. On the other hand, I focus upon the current discourse on technology, transparency, and security. I show that it encourages an uncritical acceptance of the construct of technology as a powerful yet neutral augmenting tool and the market-driven construct of technology as a solution to the current problems – whatever they are (even those that have been caused by technology itself). This can explain why technology – in spite of its huge and increasing impact upon security and intelligence practices – remains to be perceived as 'just a tool' by many practitioners. I suggest that, apart from technological tools, intelligence practitioners need conceptual tools that would enable them to critically assess the effects of specific information technologies upon their everyday practices and strategic purposes.

I then proceed to the conceptualisation of the Internet for the purposes of intelligence. I suggest that adoption of a social scientific concept of the Internet as a social space (a locus of social interaction) can usefully inform the development of reliability assessment criteria and enhance data analysis. The use of Internet sources needs to be supported by an analysis of the conditions of their production, distribution, and consumption. Also, information technologies (search engines, databases, websites, etc) need to be approached as social (discursive) practices that are both selected and selective. Social sciences can provide conceptual frameworks and analytical tools enabling security/intelligence practitioners to critically reflect upon data as being shaped by particular discourses, knowledge systems, and cultural

worldviews.

3 Technology, security and intelligence

At present, understanding of the social implications of modern ICTs in security practices is conducted mainly within legal and political discourses which aim to highlight the necessity of the balance between security and democracy (see, e.g., Strickland et al. 2005). However, the legal and political discourses tend to explain the technology's effects (both negative and positive) as dependent mainly upon the conditions of its use, thus ignoring the fact that technology can also shape those conditions. Such thinking can result in an illusion that the only and primary area of critical intervention and public control is the area of political decisions and legislations that can direct and regulate the activity of security agencies:

It is certain that information science and technology professionals are ideally situated to provide the tools and mechanisms by which the necessary domestic intelligence is collected and civil liberties are protected through established law and policy. What is different today is that the *application* of information analysis technology (i.e., knowledge discovery tools) must be managed.... (Strickland et al. 2005, p. 500, italic added).

This way of thinking is based upon a concept of technology as a *neutral tool* that augments human senses and abilities and enhances practices. The legal discourse highlights issues and factors external to the technology and naturalises the concept of technology as a neutral (although powerful) tool whose applications need to be regulated but whose intrinsic qualities are beyond questioning. This concept makes it difficult to problematise technology as yet another 'player' in the contemporary security arena and to critically assess its contribution to and effects upon specific security practices. Nor can it help find constructive *technological* solutions that may be applied to the emerging problems.

Also, the legal and political discourse is characterised by a trend to present the field of security technologies as comprising entirely of the technologies of surveillance and data collection, which is not quite so:

While technology supports all aspects of intelligence, it dominates the collection function through its role in SIGINT, IMINT, MASINT, and even the more recent construct of geospatial intelligence, or GEOINT.... But technology's reach extends beyond collection. Technology also assists in conducting intelligence analysis by helping analysts sort, manage, highlight, and share data. Modern computing and communications capabilities allow for the use of complex models – such as exploratory modelling and social network analysis – to understand multilayered relationships among people, events, and technologies. Within the realm of intelligence sharing, technology provides the foundation for expanded collaboration among analysts from diverse disciplines, agencies and

geographic locations.... Data storage, communications, collaboration tools, and data mining technologies are of particular importance (O'Connell 2005, pp. 146-147).

Nevertheless, legal discourse can create an impression that the current debates about technologies, security and intelligence address the whole spectrum of technologies and their possible applications in security practices. Such a vision can also contribute to the public and decision makers' understanding of what security/intelligence is and should be about. However, the issues highlighted within the legal and political discourses relate to one particular kind of activity – surveillance and data collection, which is characteristic of security practices aiming to obtain specific kinds of data (individuals' data that are stored in databases and relate to identities, physical appearance and observable actions). For example, in Strickland et al. (2005), *surveillance* is stated to be the primary intelligence tool and is defined as “the systematic observation or monitoring of ... places, persons, or things” (p. 434). The broad range of techniques (from covert to overt) and means (visual, aural, electronic, photographic and other) represent, nevertheless, just one kind of technological tools: they all are used for surveillance and the mining of “public or private sector databases” (p. 501). This kind of information can be quite useful in some cases but intelligence researchers (Schmitt 2005; Treverton 2003) warn against focusing primarily on this kind of data and over-reliance upon ‘hard facts’.

Technological tools that support the analysis of trends, causes and factors contributing to the emergence of threatening actors, or tools supporting collaboration and information exchange, are ‘silenced’ and technologies of surveillance and data collection are highlighted. This can result in pre-occupation with operational and tactical – rather than strategic – activities and goals. Therefore, in spite of all possible criticism and debates around surveillance and transparency issues, the legal discourse may actually contribute to the further proliferation of the practices that may potentially violate or reduce human rights, because they objectively support an already significant imbalance between different technologies and activities in the security/intelligence area (the technologies and activities aiming at data collection vs. technologies of analysis). This imbalance may result in the reproduction of an obsolete Cold War model of intelligence. This model is based upon a sharp distinction between data collection and analysis, a distinction that does not make much sense in the new conditions. This distinction significantly restricts analysts' understanding of what can be counted as useful or relevant information because it entails a positivist understanding of data as some objective facts that exist independently from the ‘observer’ (analyst) and need to be discovered. As Schmitt (2005) notes, such a positivist stance based upon “the antinomies of fact and value, scholarship and partisanship” (p. 46) has been acquired by the intelligence community in order to break from the intelligence-policy maker nexus. However, the usefulness of the positivist mindset has recently been questioned by intelligence researchers (see, in particular, Treverton 2003).

Emergence of new threats and non-traditional threatening actors results in the intelligence agencies' changing role, culture and needs. The role of ICTs is growing in these new conditions. In order to use the technological potential effectively, technology should be approached not just as a tool but as a 'participant' of the intelligence and security practices, a participant that suggests – and even imposes – socioculturally specific and ideologically loaded worldviews and conceptual frameworks. However, similarly to the legal discourse on technology and security, the dominant research discourse on intelligence for an age of information tends to construct technology as a tool that can affect upon the quantity of information but is quite neutral in relation to the quality of intelligence analysis and subsequent political and strategic decisions. The implication is that the search for the ways to improve intelligence practices focuses upon the conditions that are external to the technological tools. Researchers discuss such issues as organisational structure and ethos, mind-sets of intelligence community, relationships with policy, and legislation (Berkowitz 2005; Treverton 2003). Meanwhile, the concepts that are given to the user together with the new ICTs – e.g., the narrow-technological and /or positivist scientific concepts of the Internet, data, and reliability – need to be re-examined in the changing conditions.

The age of information is characterised by rapid technological developments and overwhelming amounts of information, which makes reshaping of intelligence an imperative, argues Treverton (2003). In today's world, intelligence business is less about collection and secrets but more about information “defined as a high-quality understanding of the world using all sources, where secrets matter much less and where *selection* is the critical challenge” (p. 98). The previously sharp distinction between *collection* and *analysis* is blurring, in particular when the Internet is used as a source of information. This creates a set of new requirements for the ‘information brokers’, such as an ability to sort “fact from fiction, or signals from noise” (p. 9). Accordingly, the consumers of intelligence information (politicians and decision makers) “need to beware of those who surf the Net but are not themselves experts: Who knows what such people might make of the Net’s mix of fact, fancy, and pure error?” (p. 10).

Although open sources are very important for today's intelligence, intelligence is returning to a preoccupation with secrets. Treverton (2003) explains why this is happening and what issues need to be addressed in order to reshape intelligence for an age of information. He points out multiple factors – starting from the intelligence ethos, professional norms and organisational features as historically shaped by the Cold War. However, this overview does not include one more important factor – the patterns of thinking embodied in technology. Treverton outlines the range of information brokers whose number and influence will be increased in the age of information, and argues that the competition between different information brokers will also increase. However, this list does not include such an important player as technology: technology is just something that is used by actors but it does not

act itself. In other words, when it comes to information technology, Treverton's otherwise quite innovative approach to intelligence for an age of information seems to be still influenced by technologists' discourse on technology. Technology is constructed as a *tool* that is used by competing information brokers rather than one more 'competitor', which means that the quality of intelligence analysis is stated to be dependent entirely upon people's expertise (or lack of it). For example, the Internet search engines are presented as tools that, while not currently able to solve the problem of information reliability on the Internet, are, without doubt, evolving towards the brighter future:

The Web is rich on sources but short on reliability. Over time, search engines will improve and help provide first-cut assessments of reliability. Still, the best Net surfers are experts who can make sense of the Net's stew of fact, fancy, and mistake (Treverton 2003, p. 104).

The discursive construction of technology as a neutral augmenting tool needs to be problematised. It is difficult to say whether such a critical enterprise could help the development of omnipotent search engines that Treverton thinks they can become.¹ At least, it can help understand that the technologies mediating access to information may be partly responsible for the fact that sometimes analysts have to deal not with meaningful information (data, knowledge) but with "stew of fact, fancy and mistake". Such a critical analysis could help the intelligence practitioners to really "keep up with advancing technology" because keeping up with technology means not only an ability to master search engines but also an ability to critically assess the Internet as a sociocultural phenomenon, and to use this meta-knowledge effectively. The intelligence community needs to be educated on the ICTs as a sociocultural phenomenon; they need to be able to critically assess the ICTs as being both selected and selective and, therefore, capable of influencing the dataset and data interpretation. Tools are needed that enable users to make this kind of critical reflection upon technologies and resources part of their meta-description of sources and data. The social sciences can help develop such awareness and can provide frameworks and tools to be used by practitioners to make more sense of diverse data (knowledge, insights) obtained from different kind of sources as well as for facilitating interaction and collaboration between intelligence practitioners.

4 Distributed intelligence: a need for meta-information

Due to the changing nature of threats and threatening agents, the mentality of the intelligence community is changing, as well as the structure of intelligence organisations. For example, Scott (2006) criticises the idea of vertically integrating intelligence collection, analysis and operations, and argues that new strategies should be developed. These strategies may require creation of *distributed intelligence* networks

¹ See also O'Connell (2005) about such expectations: "There are high expectations for science and technology in helping to solve some of the more modern aspects of intelligence, like the analyst's challenge of information overload and the visualization of complex phenomena like radar and biological data" (p. 140).

supporting exchange of information between decentralised groups with diverse skills and expertise:

It may take distributed intelligence networks to fight globally connected networks of local terrorist cells. ... Informal bonds may need to grow among diverse experts with idiosyncratic personal skills and the operational branches fighting terrorism, so that a phone call from an expert or operator in one country to another country can trigger specific responses without plodding through official channels... (Scott 2006, pp. 293–294).

What aspects of practice and technological support need to be addressed in order to enable intelligence branches to share their views and expertise? Scott (2006) highlights the importance of the organisational structure and discusses such alternatives as *centralisation* and *network*. Centralisation is not desirable and, indeed, should be avoided because it may decrease the quality of analysis:

[I]f you want to solve a novel problem in an applied field... you are more likely to succeed by consulting a decentralized group of problem solvers with diverse skills and expertise rather than a hierarchically organized group of like-minded experts who seek consensus, even if they are the best in the field (Scott 2006, p. 294).

However, the proposed organisational changes may have multiple and not necessarily beneficial socio-political consequences. Therefore, the search for a solution in technology seems to be more attractive and promising.

For such a network to be efficient, technological tools are needed that could support an effective and meaningful exchange of information between problem solvers with diverse expertise and diverse sets of data. The problem with the development of such tools (e.g., collaboration software, databases, analytical and modelling tools) is that they are largely shaped by the narrow-technological concepts of data, information, meta-data and communication. These are the concepts that technology developers (engineers, computer scientists, etc) acquire in their professional training and whose heuristic significance and utility they sometimes tend to over-generalise (Resnyansky 2002). Technological concepts and values, such as the primacy of the quantity of information over its quality and the acceptability of decontextualised pieces of information, however, are not necessarily those that make sense in intelligence practice. On the contrary, it may be the uncritical acquisition of the technological concepts and values that have contributed to the regrettable and problematic turning of intelligence analytic centres into ‘newsrooms’ and the changing nature of the products of intelligence:

[P]olicy officials seldom have time or patience to articulate their information requirements precisely. Nor do most of them know enough to task intelligence operators effectively should they find the time to try. “More on Iran” or “better stuff on Saddam Hussein’s intentions”: [sic] This is the level at which most policy officials express their intelligence

needs... By organizing the process in this way, each bit of intelligence stands by itself as a discrete commodity. Each bit can be updated, but the updating, too, comes in discrete chunks. The cycle creates the perception that the product of intelligence is “products,” most often pieces of paper (or symbols on a computer screen). In fact, by contrast, those pieces of paper are only inputs. The output of intelligence is better understandings in the heads of people who must act or decide (Treverton 2003, pp. 106–107).

The ICTs – due to their emphasis upon keyword search or the equalisation of ‘document’ and ‘content’ (without care about meaning and context) – can amplify some counter-productive aspects of the organisational structure and culture of intelligence-policy nexus, such as outlined by Treverton (2003) above. Therefore, the dominance of technological concepts needs to be questioned and the development of tools supporting intelligence analysis needs to be informed by the concepts developed in social sciences.

The concept of distributed intelligence implies that an exchange of information within the intelligence community requires a development of critical approach to information sources. The participants of such exchange need to be able to explicate and problematise their own and others’ assumptions and evaluation of sources, rather than to take them for granted. Meta-information about sources is needed so that analysts could assess others’ evaluation of the sources, rather than take for granted others’ subjective opinions about the sources’ reliability and credibility:

While technology can help make greater use of collected data, it must do so with relevant operational concepts and what might be called “metadata.” For example, though constructing a massive database with current and archival data of all types may provide a powerful tool for an intelligence analyst, it will be useless without some regard for the educational level, experience, and technical skill of the analyst who is using that database. Further, if horizontal integration is the wave of the future, it must accommodate more than a massive accumulation of data in the hope that “smoke, light, and heat” – one analyst’s description of a fully comprehensive intelligence picture – will emerge. If data are not thought about more holistically – including how it [sic] may be processed, evaluated, and understood by both analysts and decision makers – utter confusion may just as likely be the outcome. Among other issues, consideration must be given to the relative values of specific pieces of information, their real or potential error values, and their overall potential utility in providing intelligence assessment to someone with little or no experience in the exotica of intelligence (O’Connell 2005, p. 150).

The concept of distributed intelligence implies that intelligence analysts need a framework for a meaningful referencing and description of the sources that they

used. In order to support intelligence communication across organisations, states, and cultures, such a framework needs to be embodied in technological tools supporting interaction and analysis. Due to the complexity and the specific nature of data on social processes, a social sciences' contribution is required. Social sciences can help develop a meta-analytical framework that enables analysts to capture information about a broader context in which certain facts or events are embedded. They can also provide theoretical frameworks that enable analysts to identify and collect relevant data in a systematic way. Most importantly, they provide conceptual foundations and methodologies for an analysis of discourses, ideological stances, grand narratives, and commonsensical clichés that shape both the politicians and researchers' conceptualisation of the phenomena they need to know about. Specifically, the development of tools supporting intelligence analysis of political and mass violence can benefit from an integration of the body of social scientific knowledge revealing how contemporary threats of terrorism are constructed in various discursive practices – media, the Internet (e.g., blogs), official speeches, analytical papers, etc (see, e.g. Baudrillard 2002; Edwards and Martin 2004). As social research has shown, the contemporary citizen is exposed to competing constructions of terrorism that are shaped by different rhetorical themes. These constructions intend to serve the interests of particular groups and to affect how terrorism is perceived by the public, decision makers, and, to a certain degree, by researchers and analysts. Therefore, it is important that the technological tools supporting intelligence analyses could enable analysts to critically reflect on the heuristic significance of different constructions, and to approach collected data as products of multiple and biased interpretations rather than as objective decontextualised facts. Such tools can also help analysts exchange information in a more meaningful and productive way.

5 The Internet as an information source and a discursive practice

The issue of reliability is one of the most important when it comes to the use of the Internet as a source of information in intelligence. This issue has two interrelated aspects: the criteria of reliability assessment and the very legitimacy (and usefulness) of the category of reliability for intelligence activities aiming at an understanding of social actors and trends. Currently, in the intelligence area, reliability of sources can be assessed in such terms as: *almost always reliable*, *usually reliable*, *fairly reliable*, *fairly unreliable*, *unreliable*, and *cannot be judged*; credibility of source is assessed in such terms as *almost certainly true*, *very likely*, *likely*, *unlikely*, *very unlikely*, and *cannot be judged* (Pope and Jøsang 2005).² These abstract evaluative terms capture the results of practitioners' subjective perception of the reliability of information sources but do not provide any qualitative information about the sources and the logic and foundations behind analysts' reasoning. The practice of using such abstract estimative terms may be based upon an implicit assumption that the evaluated sources are of

2 For a classic exposition of estimative intelligence, see also Kent (2007).

the same nature and that all practitioners share knowledge regarding the nature of the sources. Such an assumption, however, cannot be taken for granted in the case of the Internet due to the diversity and non-homogeneous nature of the information sources that can be accessed and data that can be used.

According to Myburgh (2005), information professions developed categories for the evaluation of different information entities such as data, records, documents, information, and knowledge. Specifically, data is evaluated in terms of accuracy, validity, completeness, timeliness, auditability and integrity. Documents – in terms of format, scope of content, relation to other works, authority of author and publisher, treatment, arrangement, cost and longevity. Records – in terms of authenticity, completeness and accuracy (evidential value). Information – in terms of authority, currency and completeness. Information has a relative rather than absolute value, and is influenced by the context of use. Knowledge is evaluated in terms of ‘truth’ and validity; these depend upon methodology, type of knowledge, or knowledge framework in a discipline. These categories and evaluation criteria closely connected with the practices and ethos of the information profession and, therefore, are not universal. Categories and criteria of information sources’ reliability developed within the field of academic research are not universally applicable as well. They are shaped by specific practices of scientific research and, consequently, their applicability to and usefulness for the security and intelligence practices need to be critically re-examined.

Uncritical acceptance of technological discourse by analysts and modellers can also affect how the data are used in modelling and analysis. Specifically, it can result in treating all kinds of sources equally. For example, Weaver et al. (2006) put data from very different sources (such as news articles, web material, technical analyses, etc) into a database used in order to “characterize the terrorist organization, its ideology, political goals, campaign characteristics, operational environment, capabilities, tactics, and many other attributes” (p. 4). Sources of a different nature were then approached as a homogenous field, as if news articles, technical analyses, and web materials were written from a single perspective and had equal value as sources of factual knowledge.

The concept of the Internet as a source of information needs to be problematised because it highlights just one – and not necessarily the most relevant – aspect of this complex phenomenon. As Scott (2006) argues, the Internet needs to be approached first of all as a communication space, a virtual “market” in which social entities are emerging in the process of social interaction:

The semi-anonymity of internet communication, which lessens the compulsion to hedge and defend oneself, promotes self-disclosure and facilitates disregard of contextual differences that might otherwise distract from or hinder communication.... [T]he need to make verbally explicit one’s feelings and ideas favors disambiguation of messages and reaching mutual understanding and consensus.... A new and vibrant

Jihadist “market” is emerging, which is decentralized, self-organizing and self-adjusting (Scott 2006, p. 293).

In other words, the Internet can become yet another site of the formation of threatening identities and groups. This vision of the Internet corresponds to the postmodernist concepts of identity (Turkle 1995), literary criticism and semiotics (Bakhtin 1981, 1984; Barthes 1979, 1992), and discourse theory (Foucault 1983, 1984). This vast area of social thinking is still outside the boundaries of intelligence research, although it can provide theoretical frameworks for the development of a qualitative approach to the Internet sources (as will be shown below).

For the purposes of threat anticipation, we need to analyse not only ‘reliable’ sources but also sources that function as virtual space for social interaction and emergence of threatening agents. Although such sources cannot provide factual information, their very existence, dynamics of their appearance, number of visitors, and other characteristics provide valuable data. Therefore, it is important to approach the Internet sources in the functional terms. The purely ‘cognitive’ categories (such as *true – false, reliable – unreliable*) are insufficient and their dominance may result in ignoring the value of the Internet as a locus of pragmatic action and social interaction. An evaluation framework is needed that takes the diverse nature of the Internet sources into account and helps the information user to evaluate information sources in connection with specific fields of knowledge, institutional settings and practices, and to approach it as a locus of social interaction and identity formation.

6 Language, information, and technology

The discussion conducted above aimed at a provision of a rationale for the integration of social sciences into the development of analytical frameworks and tools supporting intelligence use of the Internet as a resource and a technological tool of information access. This section outlines theoretical foundations of a *qualitative* approach to the Internet – both as a resource and a technological tool.

The Internet is mainly about data represented in the linguistic mode. Different concepts of *language* can shape the technology developers’ and the users’ thinking about the Internet. Their thinking may be shaped, for example, by a semiotic concept of language as a code (system of signs and rules) that is used as a means of communicating ideas or feelings. This concept emphasises, however, only one – cognitive – aspect of linguistic activity. According to a functional approach in linguistics (Halliday 1985), language is used in order to offer/demand both information and service. This means that some utterances should be perceived as actions and, as such, they may be quite important even if they convey incorrect information about reality. In the case of the Internet, Jihadist websites aimed at the propaganda of ideas are examples of such kinds of utterances. Although they may be unreliable and convey untrue facts, they should not be dismissed as sources of data on this ground. However, pre-occupation with the evaluation categories informed by the cognitive/information concept of language may actually result in assigning

less value to these kinds of websites as sources of data. Meanwhile, the area of ICTs is based upon the concept of language as a code (formal systems of signs and symbols) rather than as an activity. In addition, this concept of language presents it as a 'thing in itself' (a closed system) while the functional theory of language emphasises its connection with the social and cultural context.

The Internet provides access to multiple visions that are developed, on the one hand, within scientific disciplines and, on the other hand, in media, blogs, etc. It is important to distinguish between the visions formulated within scientific disciplines and the views constructed within the field of 'doxa' (opinion). Intelligence analysts are interested in both, although they use them differently. Therefore, it is required to clearly identify the status of data in terms of production, in particular because opinion (doxa) may be disguised as a piece of research. Social researchers are quite concerned about this phenomenon (see, e.g., Horgan 2005; Schmid and Jongman 1988; Silke 2004a).

There are Internet websites (e.g., so called 'Jihadist propaganda' websites, or blogs, etc) that cannot and, indeed, should not be approached in such terms as true-false. Their primary function is not to deliver information (facts, data) but to be a pragmatic action aimed at the formation of opinions and shaping minds. They also serve as loci of social interaction and of the processes of the formation of identities, groups, and movements (Bailey and Grimala 2006; Hoffman 2006; Weimann 2006; Whine 1999a, 1999b). In the latter case, in particular, it is not secondary information about facts but 'reality', which has its value due to existential status. The propaganda websites may contain false or distorted messages but they cannot be dismissed on this ground. On the contrary, such websites are a very interesting phenomenon whose analysis can help analysts better understand the speaker and hypothesise about who the intended audience is, the audience's expectations, and what the interested agents expect or encourage this audience to do. For example, Torres et al. (2006) show that the analysis of propaganda websites can, first, help obtain an idea of the kinds of agents that are functioning in a particular area. These may be: groups that directly practice violence; those that support them morally; 'ghost' groups; and clandestine denominations specialising in the information dimension of social movements. Second, the analysis of propaganda websites can also help identify the kinds of audiences and reference groups for particular ideas (e.g., groups within/outside the domain of a political organisation; concrete or 'imagined' communities). Third, it can help obtain an idea of the means and channels of ideas' diffusion, distribution and reproduction (e.g., close/open channels, networks, and geography).

Understanding of concepts such as data, information, knowledge and information technology can affect upon the use of the Internet in intelligence. It is impossible to review these concepts in this paper. Therefore, I just note that some of the current trends and needs in intelligence can benefit from the concept of *data* in qualitative social research (see, e.g., Mason 2002). This concept emphasises that data are not given to the researcher as something that exists independently from the researcher's

theoretical assumptions and ideological stance. Rather, data are constructed in the process of research. Data, information, and knowledge are, therefore, socioculturally specific and are shaped by institutional practices and interests of particular groups. Also, as sociology of science has shown, the material aspects of knowledge production, transmission and consumption are as important as its content (see, e.g., Reid (1993) on the role of funding and network in terrorism research).

The concept of *information technologies* developed in the social theories of science, technology and knowledge (e.g., Bijker, Pinch and Hughes 1987; Ellul 1964; van House 2004) aims to highlight the social and transformative nature of technology. According to this approach, information technology and resources are not neutral; they are shaped by particular and partial views and values, are selective of both the information and the information user, and can impose certain patterns of information usage.

The sociocultural concepts of information and information technologies help the user to understand that, due to the use of IT, he/she deals not with primary information but with an information universe that has been already ordered by somebody and, therefore, it is necessary to critically assess the potential effects of that ordering. This understanding can be informed by the concept of knowledge as a social construction (Foucault 1972) and by the idea of the role of social networks within knowledge and information access (Davenport and Hall 2002; Lievrouw and Farb 2003). Within this approach, information searching is understood as a social process of becoming affiliated with particular communities and sharing concepts and discourses developed within particular domains of knowledge and practice.

However, the development of such awareness may be affected by the concepts embodied in technology – specifically, the concept of information searching formulated within the domain of information science (see, e.g., Wilson 2000). It can also be affected by the promotional discourse on ICTs. This discourse tends to present ICTs as impartial and objective. For example, databases are constructed as objective and reliable sources of information. This construction draws upon a concept of electronic reference work developed within the fields of information and library science and the publishing industry (see Armstrong and Large 1990). This concept highlights the temporal and spatial aspects of such an activity as information search. Electronic reference works are praised as having advantages described in terms of size, comprehensiveness, and up-to-date information. However, those may not all what the intelligence practitioner or a scholar working on terrorism-related problems needs. Gordon (2004a), for example, identifies two major problems that terrorism researchers encounter when they use electronic information sources, such as directory and bibliographic databases. First, they are characterised by instability: “new documents push out older documents, and the results of queries are constantly changing” (p. 87). Second, interfaces and search strategies are changing, which affects the results of the search. Gordon argues that “[t]he instability of these resources... accentuates the realistic view that information technology was and is

unable to delineate the boundary lines of terrorism as a distinct subject of research and teaching” (p. 87). This study shows that databases are not neutral technological tools or resources; they can affect upon a research field, e.g., via establishing and changing its boundaries.

Another possible effect of technologies is that the user may find it difficult to distinguish between core and peripheral research on terrorism. The use of keyword search results in that the field of research is perceived by the database user as homogenous, in which there is no division between core and peripheral subfields or between the hierarchy of scientific publications (see, e.g., Gordon 2004b; Silke 2004b). This, in turn, results in that the user may find it difficult to make a judgement regarding the reliability and authority of the sources that are accessed with the help of this technology.

Another problem with event databases is that the range of data is affected by particular methodologies and theoretical assumptions. The selective nature of event databases is, however, not obvious. Rather, the user may be misled by the databases’ descriptions emphasising the quantitative features of databases and presenting them as comprehensive sources of data in spite of the fact that those data represent only particular aspects of a phenomenon. The following description of the Global Terrorism Database³ may be considered an example of the promotional discourse on event databases:

The Global Terrorism Database (GTD) is an open-source database including information on terrorist events around the world since 1970 (currently updated through to 2004). Unlike many other event databases, the GTD includes systematic data on international as well as domestic terrorist incidents that have occurred during this time period and now includes almost 80,000 cases. For each GTD incident, information is available on the date and location of the incident, the weapons used and nature of the target, the number of casualties, and – when identifiable – the identity of the perpetrator....

Characteristics of the GTD

- Contains information on over 80,000 terrorist attacks
- The main types of information found in the GTD are items that you would expect to find in a well written newspaper story about a terrorist attack: the type of attack, the number of persons killed, the group claiming responsibility, the date of the event and so on
- The GTD is currently the most comprehensive unclassified database on terrorist events in the world
- It includes information on more than 27,000 bombings, 13,000

3 ‘Global Terrorism Database’ (2007), National Consortium for the Study of Terrorism and Responses to Terrorism, retrieved July 17, 2007, from <http://www.start.umd.edu/data/gtd/>.

assassinations, and 2,800 kidnappings

- The original data included information on over 45 variables; the new data includes over 120 variables
- More than 75 data collectors with expertise in six language groups are currently engaged in collecting GTD data
- Data collection is supervised by an advisory panel of 12 terrorism research experts
- Over 2,000,000 news articles and 25,000 new sources were reviewed to collect GTD from 1998 to 2004 alone.

As Silke (2004a) argues, although event databases are widely used in terrorism research and analysis, data collected in event databases is not very reliable since it is often based on journalistic analyses and descriptive statistics. The result of this is that terrorism research can provide rather reliable knowledge on factual details of terrorist events but is not that reliable when it comes to the explanation and behavioural patterns:

[R]esearch which emerges from the various event databases which are available... tends to be relatively good at answering questions as to the *who*, *when* and *where* of terrorist activity. Issues of *why* are not so solidly covered; and perhaps even more surprisingly the *how* of terrorist events is remarkably underexamined. (Silke 2004a, p. 10)

However, these limitations of event databases can be unnoticed due to the dominance of the promotional discourse on ICTs.

The concepts of language, knowledge, information and information technologies can be linked together via the concept of *discursive* practice developed in the linguistic and semiotic studies informed by critical social theory. This approach is developed, for example, in the works of Hodge and Kress (1988), Kress and van Leeuwen (1990), Lemke (1995) and Fairclough (1992). Within this approach, texts are conceptualised as being embedded in the processes of their production, distribution and consumption (understanding and interpretation). The processes of textual production, distribution and consumption are shaped by social institutions, cultural traditions, and communication technologies. Texts are products of a social order and power relations, and they may have the reproductive and transformative effects upon the systems of knowledge, social relations, and social identities (Fairclough 1992). Adoption of the concept of text as an instance of discursive (social) practice can help develop IT-based tools enabling the user to take context into account and to consume the Internet information sources in more meaningful ways.

If the ICTs is approached as a thing in itself, the use of ICTs in security and intelligence practices will remain to be shaped by the discourses of technological determinism and be influenced by the narrow-professional views of technology developers and/or the interests of sales people, with their specific vision of the advantages and disadvantages of ICTs. This can significantly restrain the efficiency of attempts to minimise the undesirable impact of ICTs upon security practices.

From the perspective of the war on terrorism, the imbalance of intelligence practices and technologies means that the security practitioners and decision makers will be more likely to adopt reactive rather than proactive strategies – if not always in relation to events and actions but almost always in relation to the causes and conditions of the emergence of actors that may wish to make those events occur. Thus, due to this construction of technology as a neutral tool and because of pre-occupation with the technologies and activities of surveillance and data collection, the legal and political discourses – while aiming to find ways of reaching a balance between security and individuals' rights – can actually narrow the range of strategies and means that a society can choose in order to deal with new threats effectively.

7 Conclusion

This paper has identified and critically analysed theoretical assumptions and discourses that are currently shaping public debates about the social impact of security practices and the intelligence researchers' discussion of the intelligence for an information age. These discourses promote a technological concept of the Internet as a powerful yet neutral technology of information storage and access and the market-oriented concept of the Internet as a communication medium. An uncritical adoption of such a construct of technology may have a negative impact both upon specific practices of data collection and analysis and the long-term strategies and goals. It entails positivist assumptions and epistemologies whose usefulness is highly problematic due to the specific nature of contemporary threats.

The Internet offers data/information/knowledge produced within such diverse and heterogeneous fields as academic studies, media, adversary propaganda, etc. The use of the Internet in intelligence analysis needs to be informed by an understanding of the following: (a) those sources not usually intended to be used for the purposes of intelligence; they are shaped by other practices, needs, and interests (e.g., news stories in the media aim at the promotion of certain views and ideas rather than at the provision of objective facts); (b) data and information are shaped by different discourses, knowledge systems, and cultural worldviews; and (c) access to data is mediated by information technologies and resources (databases, search engines, etc). Therefore, the use of the Internet needs to be supported by tools that enable the analyst to critically reflect upon and take into account the conditions of the data/information/knowledge production, distribution, and consumption.

Development of such tools can benefit from an integration of the multifaceted and insightful knowledge about the Internet developed within qualitative social research. It may also benefit from the use of sophisticated approaches and methodologies of data analysis developed in such areas as sociology of science, social semiotics and critical discourse analysis. These approaches can help analysts better understand ideologies and values that may be used in order to manipulate, socialise, and organise social actors.

8 Recommendations

Adoption of social scientific concepts implies that the Internet sources need to be approached:

- 1) in terms of their communicative *function* – Internet sources are divided into sources of information and space for social interaction and/or pragmatic action. These two types of Internet sources can be used differently as sources of data for intelligence analysis and modelling. Accordingly, only the first types can be assessed with the categories such as ‘true-false’ information and ‘reliable and credible’ source. Both types of sources can and need to be analysed as social (discursive) practices.
- 2) in terms of the *field* of knowledge production/consumption – disciplinary research, doxa, and propaganda. In order to use data in meaningful ways, the different kinds of Internet sources need to be categorised in terms that are specific for each field.
- 3) in terms of the *distribution* of information/knowledge. This requires an analysis of the networks and promotional techniques, and, in particular, critical attitude towards the technologies that mediate access to information. Practitioners need to be aware that the technologies can affect the intelligence practice. An uncritical perception of the IT- and market-specific discourses on technology can result in the ineffective and even counter-productive use of both information technologies and information itself. A critical assessment of technologies mediating access to information needs to be part of the use of the Internet as a source of data in the areas of intelligence and security.

The sociocultural concepts of ICTs and discursive practice can be used by intelligence practitioners in order to understand:

- What aspects/features of a website to look at?
- How to assess them as indications of the data’s usefulness and as manifestations of social practice and a particular worldview?
- How to take into account the role of the technologies and resources that mediated access to the data?
- How to capture this meta-knowledge and evaluation in a way that would facilitate – rather than slow down – exchange of information between different agencies?

References

- Armstrong, CJ & Large JA (eds) 1990, CD-ROM information products: An evaluative guide and directory: Volume 1, Gower, Aldershot.
- Bailey, TD & Grimaia, MR 2006, ‘Running the blockade: information technology, terrorism, and the transformation of Islamic mass culture’, *Terrorism and Political Violence*, vol. 18, no. 4, pp. 523–543.

- Bakhtin, MM 1981, *The dialogic imagination: four essays*, ed. M Holquist, trans. C Emerson and M Holquist, University of Texas Press, Austin, TX.
- Bakhtin, MM 1984, *Problems of Dostoevsky's poetics*, ed. and trans. C Emerson, University of Minnesota Press, Minneapolis.
- Barthes, R 1979, 'From work to text', in *Textual strategies: perspectives in post-structuralist criticism*, ed. JV Harari, Cornell University Press, Ithaca, NY, pp. 73-81.
- Barthes, R 1992, 'The death of the author', in *Modern literary theory: a reader*, eds P Rice & P Waugh, Edward Arnold, London, pp. 114-121.
- Baudrillard, J 2002, *The spirit of terrorism and other essays*, trans. C Turner, Verso, London.
- Berkowitz, P (ed) 2005, *The future of American intelligence*, Hoover Institution Press, Stanford University, Stanford, CA
- Bijker, W, Pinch, T & Hughes, T 1987, *The social construction of technological systems: New directions in the sociology and history of technology*, The MIT Press, Cambridge, MA.
- Davenport, E & Hall, H 2002, 'Organizational knowledge and communities of practice', in *Annual Review of Information Science and Technology: Volume 36*, ed B Cronin, Information Today, Medford, NJ, pp. 171-228.
- Edwards, J & Martin, RJ (eds) 2004, *Interpreting tragedy: the language of 11 September 2001*, *Discourse & Society* (Special issue), vol. 15, no. 2-3.
- Ellul, J 1964, *The technological society*, trans. J Wilkinson, Vintage Books, New York.
- Fairclough, N 1992, *Discourse and social change*, Polity Press, London.
- Foucault, M 1972, *The archeology of knowledge*, trans. AM Sheridan Smith, Tavistock, London.
- Foucault, M 1983, 'The subject and power', in *Michel Foucault: Beyond structuralism and hermeneutics*, eds HL Dreyfus & P Rabinow, University of Chicago Press, Chicago, pp. 208-226.
- Foucault, M 1984, 'The order of discourse', in *Language and politics*, ed. M Shapiro, Basil Blackwell, Oxford, pp. 108-138.
- Gordon, A 2004a, 'The effect of database and website inconstancy in the terrorism field's delineation', *Studies in Conflict and Terrorism*, vol. 27, pp. 79-88.
- Gordon, A 2004b, 'Terrorism and knowledge growth: a databases and internet analysis', in *Research on terrorism: trends, achievements & failures*, ed A Silke, Frank Cass, London, Portland, OR, pp. 104-118.
- Halliday, MAK 1985, *An introduction to functional grammar*, Edward Arnold, London.
- Hodge, R & Kress, G 1988, *Social semiotics*, Polity Press, London.
- Hoffman, B 2006 *The use of the Internet by Islamic extremists: testimony presented to the House Permanent Select Committee on Intelligence*, The

- RAND Corporation, viewed 18 May 2007, <http://www.au.af.mil/au/awc/awcgate/congress/hoffman_testimony4may06.pdf>.
- Horgan, J. 2005 *The psychology of terrorism*, Routledge, London.
- Kent, S 2007, *Sherman Kent and the Board of National Estimates: Collected essays*, viewed 3 September 2007, <<http://onlinebooks.library.upenn.edu/webbin/book/lookupid?key=olbp21035>>.
- Kress, G & van Leeuwen, T 1990, *Reading images*, Deakin University Press, Geelong, Victoria.
- Lemke, JL 1995, *Textual politics: Discourse and social dynamics*, Taylor & Francis, London, Bristol, PA.
- Lievrouw, LA & Farb, SE 2003, 'Information and equity', in *Annual Review of Information Science and Technology: Volume 37*, ed. B Cronin, Information Today, Medford, NJ, pp. 499-539.
- Mason, J., 2002, *Qualitative researching*, 2nd edn., Sage, London.
- Myburgh, S 2005, *The new information professional: how to thrive in the information age doing what you love*, Chandos Publishing, Oxford.
- O'Connell, KM 2005, 'The role of science and technology in transforming American intelligence', in Peter Berkowitz (ed), *The future of American intelligence*, Hoover Institution Press, Stanford University, Stanford, CA, pp. 139-174.
- Pillar, PR 2004, 'Intelligence', in *Attacking terrorism: elements of a grand strategy*, eds AK Cronin and JM Ludes, Georgetown University Press, Washington, D.C., pp. 115-139.
- Pope, S & Jøsang, A 2005, 'Analysis of competing hypotheses using subjective logic', in *Proceedings of the 10th International Command and Control Research and Technology Symposium (ICCRTS'05)*, McLean Virginia, USA, viewed 25 May 2007, <<http://sky.fit.qut.edu.au/~josang/papers/PJ2005-ICCRTS.pdf>>.
- Reid, E 1993, 'Terrorism research and the diffusion of ideas', *Knowledge & Policy*, vol. 6, no. 1, pp. 17-38.
- Reid, E, Qin, J, Chung, W, Xu, J, Zhou, Y, Shumaker, R, Sageman, M & Chen, H 2004, 'Terrorism knowledge discovery project: A knowledge discovery approach to addressing the threats of terrorism', *Proceedings of the Second Symposium on Intelligence and Security Informatics*, June 10-11, Tucson, AZ, pp.125-145, viewed 24 November 2006, <http://ai.arizona.edu/people/edna/AILab_terrorism%20Knowledge%20Discovery%20ISI%20_apr04.pdf>.
- Resnyansky L 2002, 'Computer-mediated communication in higher education: educators' agency in relation to technology', *Journal of Educational Enquiry*, vol. 3, no. 1, pp. 35-59, <<http://www.education.unisa.edu.au/JEE>>.
- 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), <http://www.dsto.defence.gov.au/publications/5099/DSTO-TR-1955.pdf>.
- Resnyansky, L 2007b 'Integration of social sciences in modelling: an interactionist approach to research practice', paper presented at the First International Conference on Computational Cultural Dynamics (ICCCD 2007), 27-28 August, University of Maryland, USA, <<http://www.umiacs.umd.edu/conferences/icccd2007/lucy-r.pdf>>.
- Schmid, AP & Jongman, J 1988, Political terrorism: a new guide to actors, authors, concepts, data bases, theories, and literature, Transaction Books, Amsterdam.
- Schmitt, GJ 2005, 'Truth to power? Rethinking intelligence analysis', in *The future of American intelligence*, ed. P Berkowitz, Hoover Institution Press, Stanford, CA, pp. 41-64.
- Scott, A 2006, 'A failure of imagination (intelligence, WMDs, and "virtual jihad")', *Studies in Conflict and Terrorism*, vol. 29, pp.285-300.
- Silke, A 2004a, 'An introduction to terrorism research', in *Research on terrorism: trends, achievements & failures*, ed. A Silke, Frank Cass, London, Portland, OR, pp. 1-29.
- Silke, A (2004b), 'The road less travelled: recent trends in terrorism research', in *Research on terrorism: trends, achievements & failures*, ed. A Silke, Frank Cass, London, Portland, OR, pp. 186-213.
- Strickland, LS with DA Baldwin and M Justen 2005, 'Domestic security surveillance and civil liberties', in *Annual review of information science and technology*, Volume 39, ed. B Cronin, Information Today, Medford, NJ, pp. 433-513.
- Torres, MR, Jordan, J & Horsburgh, N 2006, 'Analysis and evolution of the global jihadist movement propaganda', *Terrorism and Political Violence*, vol. 18, no. 3, pp. 399-421.
- Treverton, GF 2003, *Reshaping national intelligence for an age of information*, Cambridge University Press, Cambridge, UK.
- Turkle, S 1995, *Life on the screen: Identity in the age of the Internet*. Simon & Schuster, New York.
- Van House, NA 2004, 'Science and technology studies and information studies', in *Annual review of information science and technology*, ed B Cronin, Information Today, Medford, NJ, pp. 3-86.
- Weaver, R, Silverman, BG, Shin, H & Dubois, R 2001, Modeling and simulating terrorist decision-making: A "performance moderator function" approach to generating virtual opponents, viewed 7 September 2006, <<http://repository.upenn.edu/cgi/viewcontent.cgi?article=1026&context=hms>>.
- Weimann, G 2006, 'Virtual disputes: the use of the Internet for terrorist debates', *Studies in Conflict & Terrorism*, vol. 29, pp. 623-639.

- Whine, M 1999a, 'Cyberspace – a new medium for communication, command and control by extremists', *Studies in Conflict & Terrorism*, vol. 22, pp. 231–245.
- Whine, M 1999b, 'Islamist organisations on the Internet', *Terrorism and Political Violence*, vol. 11, no. 1, pp. 123–132.
- Wilson, TD 2000, 'Human information behavior', *Informing Science (Special Issue on Information Science Research)*, vol. 3, no. 2, pp. 49–55, viewed 23 April 2004, <<http://inform.nu/Articles/Vol3/v3n2p49-56.pdf>>

13

The Agora-Pnyx paradox

George Mickhail

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

Abstract

The avatars of the new capitalism are decreeing how the larger economy should evolve, and follow their efficient reconfigurations of human, technological and physical resources, because it adds up to more freedom. This presented the political space with the opportunity to converge with the economic space. The result was the corporatisation of government that is inherently neo-liberal (or neo-conservative) that often produced analysis-free policies. Coupled with that, was the evolution of the passive consumer-citizen. These three challenges facing our transparent society bring into question the legitimacy of a democratic process, that seems to be driven by cultural forms which celebrate personal change and indifference, but not collective progress. This paper concludes that freedom is not just an individual matter, given the complexity of the issues, such as with surveillance and privacy, so a collective response backed by intellectual analysis can effectively confront the totalising discourse of the powerful, and force its own version of reality on the public agenda.

Keywords: Agora, efficiency, Pnyx, privacy, surveillance

The processing potential of information technology has lured public organisations towards mass surveillance and has led critics to warn against ‘creeping authoritarianism’. The fear expressed there is not the one of totalitarianism – undemocratic leadership using the existing structures as a means of repression, although this fear is also expressed – but rather of a gradual, generally unnoticed and almost unconscious encroachment of individual privacy and liberty by institutions, under the auspices of improved efficiency (Angell 1995, p.331).

1 Introduction

Plato, believed in separating the Agora (economic space) from the Pnyx (political space), because he believed that need and greed enervates people’s capacity for what is just and right. This paper draws upon Plato’s idea of how society is being weakened by the machinations of need and greed that seem to expand their sphere of influence over almost all aspects of our lives. It is particularly instructive when discussing how economic rationalism, not political idealism, is shaping the debate over public policy issues, such as: surveillance and privacy. This paper explores three challenges facing our increasingly transparent society: (a) problems due to the uneasy alliance between the economic-political space, (b) evolution of the new institutional structures and the consumer-citizen class, and (c) corporatisation of government and analysis-free policy. Those challenges will be analysed to inform our understanding of their capacity to misinform analysis of public policy issues.

2 The Agora-Pnyx liaison

Technology that lowers the cost of capital for a firm is an attractive value proposition, and naturally results in reconfiguring the capital and labour resources within the firm, in favour of the technology. Airline travel had to rely on such technological developments, such as: X-Ray machines and metal detectors, when labour intensive methods of searching through the luggage and long queues of passengers were not compatible with the rapid growth in global travel and airline schedules.

The rapid expansion of airline hubs, with airlines taking control of terminal buildings and airports, meant that airline security was also part of their business, though, a non-core function. This meant that airline companies would seek the lowest bidder on their security contracts, who would also seek the minimum wage person, in order to make a little profit for themselves (CNN 2001). Comprehensive screening during peak periods often presented a conflict of interest, between profit-driven airlines trying to minimise flight delays and the responsibility the companies carry to provide security.

Airlines, like most businesses, attempt to influence federal oversight through their contributions to political candidates in both major parties. Coupled with their powerful trade organisations and direct representation, it ensured their sway over

much of the Federal Aviation Authority (FAA) policies. For example, following the TWA-800 disaster in 1996, the commission delayed the immediate implementation of the recommended baggage matching measures, because the airlines argued that it was too costly and would enrage passengers. This inept role for the FAA continued in its relationship with the airlines over the decade and leading to September 11th, 2001. The FAA would fine the airlines for security incidents and violations and the airlines would negotiate their fines and often end up paying 10 cents in a dollar for their fines, which was far cheaper than making the necessary expenditure on security enhancements recommended by the FAA.

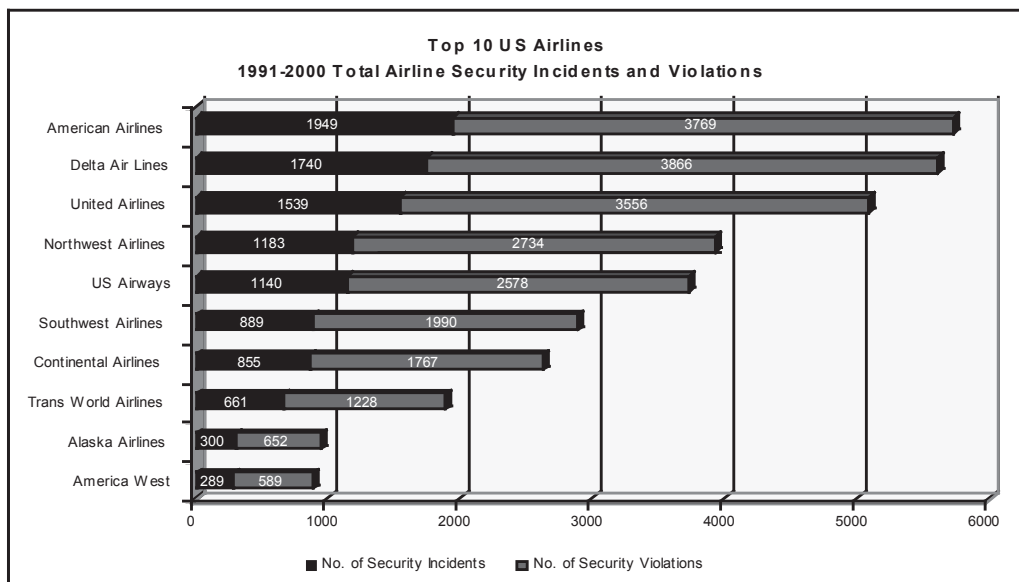


Table A – 1991-2000 Total Airline Security Incidents and Violations
(Source: U.S. Bureau of Transportation Statistics)

On September 11th, 2001 the two carriers whose jets were hijacked, were at the top of the list of airlines with security incidents and violations over a decade (1991-2000). American Airlines was the highest, with 1949 incidents and 3769 violations, and United Airlines was the 3rd highest, with 1539 incidents and 3556 violations. This perhaps highlights the dysfunctional nature of a system that was levying the same fines year after year.

It was not then surprising that Congress would come to the rescue and established the victims' compensation fund two weeks after September 11th attacks, to not only help the families of those killed and the injured survivors, but to also discourage lawsuits against American and United airlines. Those who accepted payment from the fund waived their rights to sue individual companies (CNN 2007). However, 90 families (of which 14 have decided to settle out of court on

September 19th, 2007 with terms of the settlement not disclosed) did not accept payment from the fund and sued instead the airlines and the private airline security company, Argenbright Security (released from its contract in 2002 by the Department of Transport amid allegations of inferior security standards), for their failure in their duty of care (wrongful death).

The rhetorical question is whether airlines, or other corporations, finance political campaigns of major parties, so as to wield ‘some’ influence over political oversight, given that politicians are left with no option but to offer ‘protection’ to their benefactors at the expense of the citizenry? The problem thus is with this unholy union between the economic (agora) and political (pnyx) space, which seem to privilege their interests, with the *unintended result* of a political oversight that sanctions the interests of the economic space to the detriment of the political space.

3 Citizen as consumer

The global boom in the hi-tech industry, financial services and media service organisations, which represent the new cultural ideal of the new capitalism despite being only a small part of the whole economy, exerts a profound moral and normative force as a cutting edge standard for how the larger economy should evolve. Avatars of the new capitalism proclaim that their reconfigurations of work, talent and consumption add up to more *freedom* (Saul 1997: 82, Sennett 2006:10). This is perhaps the *nexus* that brings both the economic (agora) and political (pnyx) space together in this union.

Institutions in the new capitalism are driven by an economic ideal of optimal resource allocation, through information technology, leading to maximised utility, or in short: efficiency. The quest for efficiency (Mickhail & Ostrovsky 2005: 290) is a reality involving both private and public corporations alike, where an emphasis on control over resource utilisation is done through methods of “bureaucratic accounting technology which can be coupled to totalitarian and democratic political regimes alike” (Power 1995: 293).

Power (1995: 299) argues that accounting can be regarded as a technology that subjects individuals to the ‘objectifying’ gaze of distant regulators, a system of surveillance that stimulates a style of self-regulatory behaviour. Subjects must constantly act and behave as if they are being watched and will be forced to account for themselves.

The language of asset, cost, expense, liability and profit which informs accounting is often *less precise*; its *objective* measurement of what an asset or an expense is, for example, is often dubious. Contestable profit (or loss) measurement have real consequences: share prices may fall, bank branches may be closed down, CEOs may indulge themselves with higher rewards, mass lay-offs of workers, loans may be granted, and so on. This technically ambiguous and not so readily *transparent* practice, with its abstractness from operational detail, can lead to tangible *freedoms*,

or the lack of them.

Accounting wields influence over any aspect of society that is subject to economic calculation, propounding a complex moral technology that expresses and endorses specific models of social and economic relations. Surveillance technology, chiefly used for its perceived *economic* efficiency, like accounting, whilst driven by ideals of procedural fairness and impartiality, are nevertheless dubious as to their accuracy and precision. Their ambiguous practice within society leaves room for misinformation and misinterpretation, but can also lead to material freedoms, or the lack thereof.

The social implications of such reality have been widely discussed, with the bleak warning about the erosion of privacy in the “transparent society”, due to the technological efficiency of low-cost surveillance. David Brin (1998) argues that despite the loss of true privacy, we will still have the choice between one that offers the illusion of privacy by restricting the power of surveillance to authorities, or one that destroys that illusion by offering everyone access (including the ability to observe the observers). He favors an egalitarian access to surveillance, with the public having the same access as those in power, because corrupt abuses of power would prevail without accountability and transparency.

The prevalence of the agora over the pnyx has gone one step further with not only state sponsorship of private accounting practices, but with the re-internalisation of private sector norms of business conduct (Power 1995: 298). This, to my mind, has exacerbated another shift in society: the shift from citizen to consumer.

The dominance of the economy in our daily life may help us understand how people learn to consume the new. In the past, economic inequality furnished the economic energy for politics. Strains on the economic system during the age of social capitalism produced “ressentiment” (Sennett 2006: 132). This cluster of emotions principally described the belief that ordinary people who have played by the rules have not been dealt with fairly. This intense social emotion tended to stray from its economic origins to produce resentment of old orders of patronage and privilege or minorities, such as: Jews or immigrants – who seem to ‘steal’ the social prizes to which they had no right. Under the sway of resentment, religion and patriotism were weapons of revenge.

Today, inequality is being reconfigured in terms of work experience, where symbolic analysts (Reich 1994) are at the top. The middle is fearful of being displaced, sidelined or under-used, while the bottom comprises two distinct groups. The first is the traditional working class, who was once protected by the unions and have less room to manoeuvre. The second is the immigrant class who find themselves room in a fluid and fragmented economy (Glyn 2006: 102). Ressentiment may explain why so many workers moved from the centre left to the far right translating material stress into cultural symbols.

However, Sennett (2006) argues that resentment is too narrow a way to relate economics and politics, because material insecurity prompts more than ways to

demonise those who herald unsettling change. So, instead of thinking of citizens as an angry voter, then, we might consider the citizen as a consumer of politics faced with pressures to buy.

Walmart and Carrefour are examples of the megastore that draw upon the use of advanced technology, fast-developing Chinese manufacturing practices, concentrated power at the top, disempowered unions, and has dealt with their mass workforce as if they were provisional and temporary labourers (McKinsey 2004). Consumers experience mirror centralisation of command where everything is available instantly. Sales personnel are stripped out of the consumption process as there is no need for mediation or persuasion, which as Saul (1997: 79) points out is somewhat similar to other cutting-edge bureaucracies that have stripped out their middle interpretative layer of staff, including government departments after public sector reforms in the 1980s and 1990s.

The question then becomes whether people shop for politicians the way they shop at those megastores? Has the centralised grip of political organisations grown greater at the expense of local and mediating party politics? If political leaders become instantly recognisable brands, like car models then the crux of politics becomes marketing, which is not good for political life. The very idea of democracy requires mediation and face-to-face discussion. It requires deliberation rather than packaging. However, the political version of the megastore may repress local democracy, but it may stimulate the imagination for change.

Imagination is strongest in anticipation, but it grows ever weaker through use. The new economy strengthens this kind of 'self-consuming passion' (Sennett 2006: 136) both in shopping malls and in politics. Consumption, during the 20th century, was considered to be driven by the motor of fashion and planned obsolescence. However, both of those views assumed that the consumer was passive. The new institutions (Glyn 2006: 133) with their change of work bureaucracies, from a possession with fixed content, to a position in a constantly changing network, so that work identities and institutions are continually reinvented, so they would never get used up. Hence, consumption in the 21st century thrives on the self-consuming passion.

The self-consuming passion is stimulated through active engagement in imaging (where the consumer perceives the gold-plating instead of the production-platform as the object's real value) and arousal by potency. Branding deploys platform construction on a global scale to produce the common chassis, and gold-plating to produce the small material differences, which are inflated in value. Potency is when the consumer's desires become mobilized even though they are divorced from practice. For example, how many song titles can you possibly remember from your collection of 10,000 songs on your 30GB iPod? Similarly, we buy computer software and hardware that are beyond our utilitarian needs, but it is the 'dramatisation of their potential' (Sennett 2006: 151) that leads us to desire them even if we cannot fully utilise them.

Sennett (2006: 157) poses the question: “aren’t people set free when they transcend in spirit what they directly know, use or need?” To him, the self-consuming passion might be just another name for liberty. Arendt (1998: 231) argues that in a truly democratic forum, every citizen should have the right to think aloud and debate with others, no matter their expertise. Furthermore, the test of utility and practicality should not rule either, as this test emphasizes what is rather, than what might be. Her argument, in a sense, is similar to Sennett’s view of the consuming passion, as a precondition to freedom and democracy.

The consuming passion brings focus on what is really missing in the hope for progressive change: an understanding of the profoundly ‘enervating’ role that illusion plays in modern society. The illusion (Brin 1998) of giving the power of surveillance to either the authorities or everyone is perplexing, because we do not limit what we want from surveillance to what we can actually do with it. Similarly, we do not limit what we want from the illusion of privacy or accountability to what we can actually do with them. Angell (1995: 331) observes that it is rather difficult to establish what exactly constitutes an infringement of privacy, let alone how it constitutes an attack on freedom. These confounding illusions may actually contribute to our own passivity. Sennett (2006: 161) identifies five ways in which the consumer-citizen is turned away from progressive politics (the belief that citizens are bound together in a common project, such as: privacy, limiting surveillance, accountability, and so on) and toward this more passive state:

1. Consensus politics, where we are offered political platforms which resemble product platforms (generally, they tend to be business friendly, socially inclusive and immigrant ambivalent). For example, wider surveillance powers of immigrants from Muslim countries may be a shared political platform for either side of the political spectrum. After all, either side of the spectrum are immigrant ambivalent, especially from the Muslim world after September 11th, 2001.
2. Gold-plated differences, where a re-contextualisation of the fact may take place. For example, making Muslims in their totality a terror threat, despite of the fact that the majority are law-abiding citizens. This may justify the expansion of surveillance powers given their broader presence in our society.
3. We are often asked to discount the “twisted timber of humanity”, a phrase coined by Kant. For example, surveillance technology discounts our individual complexity, where Muslims from the Middle East may speak Arabic but the dialects are quite different within each country let alone the different countries. Imagine the number of computerised Arabic interpreters to decipher taped phone conversations.
4. We tend to credit more user-friendly politics, where consumer-citizens disengage from difficult issues by comparison to craftsmen-citizens who would like to understand how things work, so they engage with difficult and resistant issues. Democracy requires citizens to be willing to make an effort to find out how

the world around them works. The consumer-citizen tends to disengage from difficult and complex issues, such as: privacy and transparency. Additionally, technological overload prompts disengagement, so one can imagine the cognitive impact of the technological jungle of surveillance.

5. We continually accept new political products on offer. For example, modelling reform on advanced business practices breeds anxiety (psychoanalysts call it ontological insecurity: fear of what will happen even if no disaster looms. It is also called: *free-floating* to indicate that someone keeps worrying even if s/he has nothing to fear in a specific situation). Another example is the anti-terror warning around cities such as with the slogan: “if you see something, say something”, which is plastered around train stations and billboards.

This shift in our role from an engaging citizen to a passive consumer-citizen is a product of the convergence of both the economic and political space, with the former dominating the latter. This brings into question the legitimacy of a democratic process that seems to be driven by cultural forms which celebrate personal change and indifference, but not collective progress. The question then would be—should we be at all concerned about this malaise of the consumer-citizen phenomenon?

4 The analytics of complexity

The convergence of both the economic and political space has brought another malaise to bear on society and the democratic process, namely: the corporatisation of the public service (Saul 1997: 76). It was a calculated assault on the independence of public servants, which hindered any meaningful analysis on policy, regardless of whether it may be contrary or not, to the policy line of the government of the day.

It is instructive to reflect on the Thatcher years of public reform to understand the machinations of public policy ‘reform’. David Willetts (1987: 445) provides an illuminating account of such change, while he was a member of the Prime Minister’s Policy Unit. Mrs Thatcher disbanded the *fifteen* members of the Central Policy Review Staff (CPRS) and replaced them with *eight* members comprising the Prime Minister’s Policy Unit in 1983.

Unlike the CPRS, the Policy Unit did not undertake long-term or large-scale studies, but rather offered policy advice on ‘current’ matters of concern, with deadlines ranging from an hour to few days. More importantly, the advice did not go to Cabinet for rebuttal or debate by departmental ministers. It was for her eyes and ears only, given that the Prime Minister’s Policy Unit was not a Cabinet Office body serving all of Cabinet, like the CPRS.

The composition of the Policy Unit in 1986 was at eight or nine, with at least three members on secondment (Willett 1987: 546) from large private sector organisations, such as: McKinsey’s, Consolidated Gold Fields and Shell, advising on their respective specialisations (and possibly their corporations’ interests). A fourth was a retired senior partner from Coopers & Lybrand. The rest were civil

servants and a university professor. Rosenhead (1995: 309) argues that her Policy Unit “did not, could not, originate the flood of radical but untested policy ideas” which reached Cabinet, as many emerged from right-wing think-tanks, and the Policy Unit was simply the messenger. Rosenhead (1995: 311) explains the ‘robust simplicity’ by which those think-tanks justified their policies.

It starts with strong value assertions and then proceeds directly to detailed prescriptions. Argumentation is intuitive (with a ‘public choice’ flavour), and proposals are not costed or quantified. There is appeal at most to anecdotal evidence, but certainly not to research.

One very ‘unpopular’ policy, which was announced in a glare of publicity, and without advanced notice to the relevant departments, was the Poll Tax.

The preceding account of events seems hauntingly familiar, not just at federal or state governments in Australia, but wherever economic rationalism is dominating public policy discussion. There has been a catastrophic retreat from reason in public affairs, in which a quasi-mystical ideology attributes magical powers to the markets (Saul 1997: 80, Stiglitz 2002: 138, Glyn 2006: 77). Since the collapse of the Soviet Union, this ideology has gone far towards establishing a hegemonic hold in the form of neo-liberal regimes in the UK, USA and Australia, which manifests a centrist political platform, which enabled economic development friendly to globalisation, flexibility and meritocracy (Sennett 2006: 163, Stiglitz 2002: 53).

Markets are thought to be correcting government malfunctions (rather than vice versa). No matter that, in so many instances of infrastructure privatisation, such as: electricity and water, the most convoluted socio-economic reengineering can only produce “a market which is artificial, rigged, imperfect and imperfectable” (Rosenhead 2006: 313). For the uncritical mind that dwells with fervour for intelligent design, the market is seen as a ‘pseudo-natural’ phenomenon, which substitutes for the exercise of collectively rational choice. The elevation of the market to almost divine, omnipotent, omniscient status has been at the expense of the down-grading of rational choice based on analysis. It is of no surprise then, that hyper debate concerning public policy issues such as surveillance is taking on similar omniscient status inflating surveillance into überveillance (Michael & Michael 2006: 361).

Setting public policy is a complicated business. Porter (1987: 87) outlines the difficulty facing the US President and others in positions of comparable authority:

They are expected to make a large number of decisions about issues on which they themselves are not expert, and therefore they are going to rely on the other people for information, for analysis, for structuring alternatives and for an assessment of the advantages and disadvantages associated with the alternatives. Many of the issues coming at them, and on which they are expected to decide, are interrelated, in the senses that what they decide on issue A today will affect the choices, and the relative

attractiveness of those choices, on issue B, C and D that they are going to be considering two weeks, three months or a year from now. Rosenhead (1995: 316) rhetorically asks the question of how can diversely interested parties, many of them largely excluded from influence, become active and effective advocates in public debate when analysis-free policy is on offer? He believes that data and information are no longer sufficient, in such an information-rich and complex world, to have power over one's own life. Rather, 'analytic capability' (Rosenhead 1995: 308) would help us shape, discard and manipulate information in order to understand our situation, devise an appropriate strategy, and advance convincingly our own *problematique* or to garner support for our causes or to undermine or demolish competing propositions.

Freedom, then for Rosenhead (1995: 319), is not just an individual matter. The complexity of issues in our world, are no longer affecting social life details but predominantly its structures and opportunities. Individualised responses are ineffectual, when only collective responses backed by critical analysis can effectively confront the totalising discourse of the powerful, and force its own reality on the public agenda.

5 Conclusion

This paper outlined three challenges facing the transparent society, when discussing some of the issues associated with surveillance and privacy. Firstly, the unholy union between the economic and political space is problematic, because the *unintended effect* of this alliance is often political oversight that sanctions the interests of the economic space to the detriment of the political space.

Secondly, the evolution of the passive consumer-citizen shaped by their experience of the new institutional structures. The shift in our role is a direct product of the convergence between the economic and political spaces, with the former dominating the latter. Surveillance technology, among other issues of public concern, chiefly used for its perceived *economic* efficiency, are nevertheless dubious as to their accuracy and precision, given their ambiguous practice within society, which leaves room for misinformation and misinterpretation.

Thirdly, the corporatisation of government and analysis-free policy is yet another malaise from the economic-political convergence. In order to be involved in the democratic process, one needs to be able to *analyse* the information that may affect one's own interests. Obviously, this is quite problematic in an information-rich society, given the information quagmire that we have to sort through. Hence, the right to information is of limited use by itself, for any effective involvement in the democratic process.

In conclusion, the discussion of those challenges brings two points to the fore: the right to analysis, and the passive citizen-consumer. Having the right to information about our privacy or the lack thereof, for example, is not sufficient for us to be involved in any discussion concerning its potential use. Having the right to analysis

is paramount for us to do so, but we must be willing to seek that right. Today, we have a better opportunity in having access to better analytical tools through the internet. The paradox of our time might be if the passive citizen-consumer will be 'bothered' to seek the right to analysis, so as to be able to engage in the democratic process.

References

- Angell, A & Laidler, P 1995, 'Information Technology and Freedom', in LSE on Freedom, ed. E Barker, LSE Books, UK.
- Arendt, H 1998, *The Human Condition*, University of Chicago Press, USA
- Brin, D 1998, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Perseus Books, USA.
- CNN Special Report on Airport Security 2001, *In-Depth Report: Flight Risk*, viewed 20 November 2001, <<http://www.cnn.com/SPECIALS/2001/trade.center/flight.risk/stories/part1.mainbar.html>>
- McKinsey Global Institute 2001, 'US Productivity Grown, 1995-2000,' Section VI, 'Retail Trade,' viewed 17 September 2007, <<http://www.mckinsey.com/knowledge/mgi/productivity>>.
- Michael, MG & Michael, K 2006, "National Security: The Social Implications of the Politics of Transparency", *Prometheus*, vol. 24, no. 4, Routledge.
- Mickhail, G & Ostrovsky, A 2005, "The MetaCapitalism Quest", *American Academy of Business Journal*, vol. 6, no. 1, pp.290-298.
- Nneji, N 2007, *14 families of 9/11 victims settle suit*, viewed 19 September 2007, <<http://www.cnn.com/2007/US/law/09/18/sept.11.lawsuits/index.html>>.
- Porter, R 1987, 'The United States' in *Advising the Rulers*, ed. W. Plowden, Blackwell, UK.
- Power, M 1995, 'Reconnecting accounting to the problem of freedom', in LSE on Freedom, ed. E Barker, LSE Books, UK.
- Reich, R 1994, 'The revolt of the anxious class', viewed 18 September 2007, <<http://www.dol.gov/oasam/programs/history/reich/speeches/sp941122.htm>>.
- Rosenhead, J 1995, 'Liberty! Fraternity! Analytic Capability!', in LSE on Freedom, ed. E Barker, LSE Books, UK.
- Saul, JR 1997, *The Unconscious Civilisation*, Penguin Books, Australia
- Sennett, R 2006, *The Culture of the New Capitalism*, Yale University Press, New Haven, USA.
- Stiglitz, J 2002, *Globalization and its Discontents*, Penguin Books, USA.
- Willetts, D 1987, 'The Role of the Prime Minister's Policy Unit', *Public Administration*, vol. 65, no. 4, pp.443-54.

14

Something smart going on: the apocalyptic aesthetics of surveillance

Marcus O'Donnell

Associate Lecturer, School of Journalism and Creative Writing, University of Wollongong

Abstract

This paper analyses surveillance as an integral element in contemporary discourses of the apocalyptic. It outlines a model of the apocalyptic that has its roots in the western religious tradition particularly the last book of the Christian bible: The Book of Revelation. It explores the intersecting narratives of surveillance, the apocalyptic and the forensic as a way of contextualising contemporary political, pop cultural and technological events. Each of these narratives play themselves out through a dialectical logic: surveillance is seen as bringing both intrusion and protection; the apocalypse is harbinger of both destruction and a new world; while the forensic revels in both discovery and horror. Each of these narratives is related to a search for meaning and authenticity and each is expressed through a broad range of multimodal contemporary mythic structures in news, film, television and politics.

Keywords: apocalyptic, surveillance, forensic aesthetics, myth

1 Introduction

Walking down the street, getting money from a bank ATM, entering a building, countless times every day we are warned by signs: “You may be photographed while...”. The intensity of this visual surveillance is matched by the voice heard every time we queue for a telephone service: “This call may be monitored for...” The technological eye and ear have become ubiquitous parts of our everyday.

A recent study calculates that if you live in London – the most surveilled of modern cities – you will appear on camera some 300 times a day just going about your normal business. (Van Melik et al 2007:26). The London CCTV system – one camera per 15 inhabitants – played a starring role in the media stories of the capture of those associated with the so-called July 2007 “Doctors Plot” which saw failed bombings in London and Glasgow. A *Time* magazine report on the bombings referred to “London’s wondrous surveillance system” and quoted U.S. Senator Joe Lieberman’s praise of that system:

“The Brits have got something smart going. They have cameras all over London... I think it’s just common sense to do that here much more widely.” (Ripley 2007)

What once would have been tagged “Orwellian” is now called “wondrous” and lauded as “common sense”. In fact in an age where “Big Brother” has become a global brand quite different to the one George Orwell predicted in his totalitarian allegory *1984*, it is hard to know exactly what Orwellian is anymore. This is indicative of an increasingly complex, shifting cultural landscape that can only be understood by looking at a range of intersecting cultural narratives.

This paper explores the intersecting narratives of surveillance, the apocalyptic and the forensic as a way of contextualising contemporary political, pop cultural and technological events. Each of these narratives play themselves out through a dialectical logic: surveillance is seen as bringing both intrusion and protection; the apocalypse is harbinger of both destruction and a new world; while the forensic revels in both discovery and horror. Each of these narratives is related to a search for meaning and authenticity and each is expressed through a broad range of multimodal contemporary mythic structures in news, film, television and politics.

I will argue that understanding the contemporary aesthetics of surveillance is essential to understanding the cultural work of surveillance technologies. Firstly I will situate surveillance within the myth of the apocalyptic. Secondly I will look at how these ideas are played out in contemporary television and film through what Ralph Rugoff (1997) has called “forensic aesthetics”. I will conclude with some brief reflections on how these ideas relate to the current news context and national security.

2 The Apocalyptic

Apocalypse – Greek for revelation – is the name given to the final book of the

Christian bible,¹ a highly symbolic end-time narrative of “blood-drenched scenes of nature gone deadly, war, and famine” (Quinby 1999:283). Images from this book – such as the four horsemen of the apocalypse who bring famine and plague and Armageddon, the site of final conflict between the forces of good and evil – are familiar motifs of popular culture. But the apocalyptic story is not just catastrophic it is also freighted with utopic millenarian promise rooted in the prophecy of the thousand-year kingdom of the saints (Rev 20:1-7) and the restoration of the holy city of Jerusalem. It is a story of redemption and transformation butted up against condemnation and destruction. It dramatises the dialectic between hope and fatalism, the end and the beginning, annihilation and transformation.

Scholars have long argued about what defines apocalypses as a genre (Webb 1999) but the generic definition of these ancient texts is relatively simple when compared with broader issues such as defining “apocalyptic ideology” or “apocalyptic movements”. What is undisputed however is the reach, the influence and the ongoing power of the ideas, beliefs and rhetorical devices that trace their lineage to this biblical book and its genre.

The apocalyptic is a theme that has been studied widely across a range of disciplines including: history (Cohn 1970;) sociology (Robbins and Palmer 1997) literature (Ahearn 1996; Kermode 2000) rhetorical studies (O’Leary 1994) cinema studies (Sharrett 1993; Dixon 2003) visual art (Cunningham and Grell 2000) and postmodern philosophy (Dellamora 1994).²

In both subtle and not so subtle ways the apocalyptic retains much poetic, religious and political power and is an influential individual and collective ordering force. The most obvious dimension of this influence can be seen in connections between the many current discourses of crisis – the war on terror, environmental collapse, threatening epidemics such as SARS and HIV – and the common understanding of the apocalyptic as cataclysm. Although the Christian apocalyptic forms the main context for this study it is important to note that the biblical story is not an isolated work it belongs to a genre of ancient middle eastern texts that deal with similar issues and share similar literary forms (Hultgard 1998). It could in fact be argued that the clash of competing Jewish, Christian and Islamic apocalyptic narratives is fundamental to understanding contemporary international relations and national security. (Gorenberg 2000; Juergensmeyer 2001; New 2002).

In this context I have previously argued (O’Donnell 2005) that the rhetoric of

1 The last book of the New Testament is also known as Revelation or The Revelation of John. It is thought to have been composed at the end of the first century CE. Its author is identified as John – “your brother who shares with you in Jesus the persecution and the kingdom and the patient endurance...on the island called Patmos because of the word of God and the testimony of Jesus” (Rev 1:9). Traditionally this “John” has been associated with the apostle John also the reputed author of the fourth Gospel. Although the exact authorship of these Johannine texts is disputed by contemporary scholars, the book is thought by some to have emerged out of a “Johannine” school within the early church, while others point to affinities with the Pauline and Synoptic traditions. (Schussler-Fiorenza 1998: 85-113)

2 This is obviously only a brief noting of select key works

George W. Bush in his construction of the war on terror and homeland security is firmly rooted in the apocalyptic religious world-view. In a radio address to the nation on September 15 2001 Bush began to establish a pattern in his war on terror rhetoric. Comforting and challenging a nation in shock from the attacks on the twin towers he quickly established that moment as an ongoing conflict and reiterated that it would be “a different kind of conflict against a different kind of enemy”.

This is a conflict without battlefields or beachheads, a conflict with opponents who believe they are invisible. Yet, they are mistaken. They will be exposed, and they will discover what others in the past have learned: those who make war against the United States have chosen their own destruction.

Underlying this implied promise of victory was this presidential caveat: “We have much to do and much to ask of the American people. You will be asked for your patience, for the conflict will not be short. You will be asked for resolve, for the conflict will not be easy. You will be asked for your strength, because the course to victory may be long.” This rhetoric of test and endurance is strikingly similar to the calls at the beginning of the *Book of Revelation* in the seven letters to the seven churches to whom the book is addressed:

I know your works, your toil and your patient endurance. I know that you cannot tolerate evildoers...I also know that you are enduring patiently and bearing up for the sake of my name, and that you have not grown weary. (Rev 2:2-3)

To the “saints” who endure is promised a crown, a white cloak and a new name written in the book of life. The specific echoes of the language of *Revelation* and its promises would have been heard by many of Bush’s Christian base and the generic language of national mission familiar from American frontierism (West & Carey 2006) meant that its power was not lost on others.

David Domke (2004) in an analysis of Bush’s speeches for the eighteen months following September 11 notes a concentration on “moment and mission”. He argues that this crisis discourse contributes to what he calls the Bush administration’s “political fundamentalism”. Calls for *imminent action* and *enduring commitment* create a strategically powerful discourse. He writes:

When combined these time focused emphases become politically potent: They allowed the administration to push for immediate action on specific policy goals [Patriot Act; establishment of Homeland Security Department; doctrine of pre-emption] with others’ questions dismissed, and to justify these desires as unchallengeable steps in a God-ordained, long term process. (2004:64)

In the next part of this paper I want to explore three other less obvious but not unrelated aspects of the rhetoric of the apocalyptic that also have telling implications for current discourses of national security and surveillance. Firstly I will look at a set of ideas that cluster around, sight, secrets and surveillance in the context of what

Lee Quinby (1994) has called the techno-apocalypse. Secondly I will look at the visceral embodiment of these ideas in what Tina Pippin and other scholars (Pippin 1999; Gomel 2000) have called “the apocalyptic body”. Thirdly, both these ideas are related to one of the central images of the apocalyptic literature: the Beast and his mark.

3 Strange things

From the opening verse of the *Book of Revelation* we know that this text is about secrets: a “revelation” of strange things that “must soon take place” made known by a message from an angel. (Rev 1:1) As the visionary journey unfolds the extent of access is also revealed:

After this I looked, and there in heaven a door stood open! And the first voice, which I had heard speaking to me like a trumpet, said, “Come up here, and I will show you what must take place after this.” At once I was in the spirit, and there in heaven stood a throne, with one seated on the throne! And the one seated there looks like jasper and carnelian, and around the throne is a rainbow that looks like an emerald. (Rev 4:1–3)

Readers of this text are invited into a secret world – through a door into heaven – they are given access to esoteric knowledge but they are also shown how deeply forces conspire in the unfolding of the cosmic drama. Gerard Von Rad argues that one of the messages of Jewish apocalyptic writing is that “the last things” can be known and exactly calculated but that this knowledge is only open to the initiated, this is why the key textual device of this genre is the esoteric cipher. The gnosticism of these texts goes to the heart of the apocalyptic world view: “He who understands the secrets understands what holds the world together in its inmost being” (Von Rad 1975:302).

The other side of this access to mysteries and esoteric knowledge is the knowledge that you too are known, fully known. The one who grants access to this new knowledge is “the one who searches minds and hearts, and...will give to each of you as your works deserve” (Rev 2:23). The story of revelation is one of both secrets and surveillance.

The seven letters to the seven churches to whom *Revelation* is addressed all follow a set formula. The refrain of these letters is: “I know.” The Son of Man whose eyes are like a flame of fire sees all, knows all and judges all: “I know your works...I know your patient endurance...but I also have this against you...For those who conquer I promise...” Surveillance, endurance and promise form the rhetorical rhythm of the *Book of Revelation*. As Henry Maier puts it:

As the readers travel with John to the heavenly throne room, where he unveils to them a vision of a slain lamb with seven horns and seven eyes, “which are the seven spirits sent out into all the earth,” the audience, already revealed to itself in the seven letters, knows that it has entered

a world of perfect universal surveillance. It responds to John's unfolding visions as an observed audience. This depiction of an all-seeing God is a commonplace in both Jewish and early Christian apocalyptic literature. The omniobservant eye of God serves as a hortatory device to guarantee obedience in the face of coming or threatened judgment against evildoers. In apocalyptic plots of the end of the world, God plays a character who sees, records, and rewards or punishes all human actions. (1997:141)

This "omniobservant God" is at the heart of what Quinby calls the "twin millennial pillars of dread and desire" (1999: 284): the desire to know and embrace the great cosmological secret and the simultaneous dread of being completely known and thus perhaps judged unworthy to share in the promise of that secret world. These dual apocalyptic impulses are deeply entrenched in western culture, and play out across three different modes of contemporary apocalyptic thinking: the divine apocalypse, the technological apocalypse and the ironic apocalypse (Quinby 1994: xv-xvi). The divine mode includes both fundamentalists from the American right as well as Latin American proponents of liberation theology. The ironic mode reflects the nihilistic and absurdist tendencies of post modern philosophy. The technological mode includes both narratives of technological devastation (from nuclear to environmental) and technological salvation (from life saving technologies to visions of a utopic world order).

4 Techno-apocalypse and the Beast

Although Quinby's three apocalyptic modes are a useful typology, she herself notes that expressions of the apocalyptic often cluster across modes with surprising effects. One of the reasons why the apocalyptic is such a buoyant form – expressing itself in movements as diverse as dissenting religious movements in the European middle ages (Cohn 1970) the Puritan settlement of America (Boyer 1992) and the Russian revolution (Rowley 1999) – is the almost viral way it combines and recombines across these various modes of expression.

The techno and divine modes have converged in recent years in a variety of significant ways. This was particularly notable in the countdown to the year 2000. A number of scholars have noted (McMinn 2001; Tapia 2002; Schaefer 2004) the convergence of techno and divine apocalyptic in discourses surrounding "Y2K" computer systems meltdown. These studies throw some light on apocalyptic attitudes to both earthly and heavenly technologies of surveillance.

Many respondents in Tapia's study of the "millennialist" Christian response to Y2K, saw technology as an "evil" force that fragmented society. They argued that it was an "idol" that turned people away from God. (278). Schaefer points out that although many "evangelicals evidently feared that society's increased dependency on technology...might usher in worldwide domination by the Antichrist... their stance toward globalism and technology is both paradoxical and ambiguous. Committed

to spreading their message by every (legitimate) means possible, evangelicals do not hesitate to employ technological advancements in production, mass communications, and travel to help them reach their goal.” (Schaefer 2004:98)

This ambiguous relationship between millennial evangelicals and technology can be also seen in one of the most popular contemporary mass communications of the apocalyptic: the best selling *Left Behind* series of “prophecy novels” from evangelical leader Tim LaHaye and novelist Barry Jenkins. The twelve part series fictionalises the events of the *Book of Revelation* narrating the last days after God’s chosen are “raptured”³ up to heaven and non-believers and not-quite-right Christians alike are left behind to endure the “tribulation” or the reign of the Antichrist.

The series is something of a publishing phenomenon. The first novel was published in 1995 and several novels in the series have topped the bestseller lists. According to *Newsweek* (Gates 2004) the events of September 11 boosted the sales of the 2001 instalment, *Desecration*, which became the best selling novel of that year. Presales of the final instalment published in 2004 reached 2 million and all up the series has sold some 62 million copies.

At the heart of the series is the work of the Tribulation Force who spearhead an underground resistance movement that battles the Antichrist and his “council of ten”. In his analysis of the novels Glenn Shuck (2005) points out that surveillance technologies are integral to both the work of the Antichrist and the Tribulation Force. He contrasts LaHaye and Jenkin’s “beast system” with the “network culture” of social theorist Manuel Castells and shows how both the Antichrist and the Tribulation Force display implicit understanding of the interaction between, new technologies and new decentralized flows of global capital.

The success of the Tribulation Force depends on its ability to clone vital components of the network culture – the Beast system it seeks to resist. Operatives require flexibility, the latest technologies, ultra modern weapons, mobility and a decentralized organizational logic. They even understand image and the possible benefits of deception in a world characterized by confusion and uncertainty. (Shuck 2005:110)

The image of the Beast that both Shuck and the authors of *Left Behind* rightly take as a metaphor for the totalizing power of the anti-God forces of apocalyptic times is a key symbol in the *Book of Revelation*. There are two Beasts referred to in chapter 13, the first Beast rising from the sea and the second Beast rising from the land. The first Beast has ten horns and seven heads and immediately assumes an irresistible position of power in the complex mythological system of *Revelation*:

One of its heads seemed to have received a death-blow, but its mortal

3 The idea of the rapture proposed by some Christians does not come from the Book of Revelation like most other key elements of apocalypticism but is based on a literal interpretation of 1 Thessalonians 4:16–18: “For the Lord himself will descend from heaven with a cry of command, with the archangel’s call, and with the sound of the trumpet of God. And the dead in Christ will rise first; then we who are alive, who are left, shall be caught up together with them in the clouds to meet the Lord in the air; and so we shall always be with the Lord. Therefore comfort one another with these words.”

wound had been healed. In amazement the whole earth followed the beast. They worshiped the dragon, for he had given his authority to the beast, and they worshiped the beast, saying, “Who is like the beast, and who can fight against it?”....Also it was allowed to make war on the saints and to conquer them. It was given authority over every tribe and people and language and nation, and all the inhabitants of the earth will worship it, everyone whose name has not been written from the foundation of the world in the book of life of the Lamb that was slaughtered (13:3-8)

This introduction of the Beast couples him with the Dragon previously identified with Satan (12:9) and places his power over all the earth in the context of an earlier battle between the forces of God and the forces of Evil staged in the previous chapter. The second Beast has “two horns like a lamb and it spoke like a dragon” and it acts as the lieutenant of the first Beast forcing all to worship this master. It is this second Beast that inaugurates the “Beast system”: the mark of the beast that attributes all economic and social status to those who are marked as followers.

It performs great signs, even making fire come down from heaven to earth in the sight of all; and by the signs that it is allowed to perform on behalf of the beast, it deceives the inhabitants of earth, telling them to make an image for the beast that had been wounded by the sword and yet lived; and it was allowed to give breath to the image of the beast so that the image of the beast could even speak and cause those who would not worship the image of the beast to be killed. Also it causes all, both small and great, both rich and poor, both free and slave, to be marked on the right hand or the forehead, so that no one can buy or sell who does not have the mark, that is, the name of the beast or the number of its name. This calls for wisdom: let anyone with understanding calculate the number of the beast, for it is the number of a person. Its number is six hundred sixty-six. (13:13-18)

For the original audience of *Revelation* the Beast had a clear lineage that linked to both similar figures in Jewish mythology and the imperial cult of the Roman emperor. Thus they understood the Beast in both cosmological and localized political terms (Schussler Fiorenza 1991:82-87). In the Middle Ages the Beast was linked to the Antichrist figure who become a vital part of the apocalyptic legend (Rusconi 1998). Both the figure of the Beast and the Antichrist still function today as a lightening rod for cosmological and political conspiracy. Google searches will identify numerous current candidates for the Antichrist including the Pope, Barak Obama, George Bush and Vladimir Putin. This game of spot the Antichrist has a long tradition from the writings of Joachim de Fiore and Nostradamus to contemporary conspiracy websites and feeds the rhetoric of secrets and signs that I have argued is essential to an understanding of the apocalyptic. This vision of the Beast and the Beast System also clearly mirrors the you-are-with-us-or-you-are-with-the-terrorists

language of the war on terror. In the mythological system envisaged in this chapter of *Revelation* those remaining in the end times belong to one of two groups, those marked by the Beast and those whose names are written in the book of the Lamb. These positions are irrevocable and these marks of identity are indelible.

The *Left Behind* authors re-envisage this web of power and the mark of the Beast in quite a specific form which clearly links to both contemporary Christian and broader fears about technological intrusion and domination. They describe the mark not as the traditional number of the beast but as a tiny microchip inserted under the skin. Shuck (2004) summarises the functions of this Beast chip:

First, it permits believers to participate in Antichrist's economy, using their implanted chips as debit cards which eliminate fraud and speed transactions. Second, the mark gives its bearer a sense of place, specifying one of ten regional kingdoms as the bearer's homeland. Third, it conveys a permanent identity which cannot be effaced. It instantly identifies one to authorities, and suggests where one belongs, allowing Antichrist's forces to track citizens and make his kingdom more secure. Fourth, every mark bears the name of Antichrist. Finally, Antichrist displays a remarkable knowledge of consumer preferences, making provision for those who want a customized, vanity design. (54-55)

However in spite of the impressive reach of the "beast system" Shuck shows that the active resistance of the Tribulation Force introduces a new kind of post rapture activism not seen in earlier prophecy novels. He points out the "naïve" faith the authors place in the skills of the heroes to outwit the vast technological resources available to the "one world government" controlled by the novels' designated Antichrist figure Nicolae Carpathia. This is largely achieved through several well-placed moles within the Beast system. The authors' "focus on individuals acting against powerful structures may serve them textually – to a limited extent....but its wisdom appears dubious outside the realm of prophecy fiction" (107). This post rapture activism sits oddly with traditional apocalyptic ideas of fated destiny but sits well with the contemporary emergence of the politicized evangelical religious right and is cognizant with a view of apocalypticism as a mobile mythic cluster that can be successfully reconfigured by believers to bouy-up their current needs and concerns. In her reader ethnography of the *Left Behind* series Amy Frykholm (2004) notes the way the novels' framing of technologies is affecting evangelical reader's fears of technology and like Shuck she notes a developing commitment to activist millennialism: "many readers identify with the Tribulation Force as a group....a community that will overcome the isolation, competition and fearful complexity of the modern world...Jason [a reader] imagines himself not as an individual hero but instead as 'part of a secretive organization'." (129)

These narratives, however naïve, allow readers to project themselves into an increasingly complex world as actors. In both the early Christian narratives of the apocalypse and in their contemporary manifestations, secrets, signs and surveillance

are essential rhetorical motifs as well as essential technologies in the divine economy of the end. These secret ciphers are embodied in particular marks of the Beast and the Lamb. The hortatory function of an omniobservant God is clear, and such a theology brings with it a particular apocalyptic subjectivity of faithful endurance – and increasingly it would seem of active engagement – which parallels more contemporary paradigms of authenticity. For millennialist Christians, those who live well under the all knowing gaze of God are seen to be living authentically: in sync with the deepest secrets that will be revealed to all at the end times. This authenticity, can now be conceptualised as a participatory event within the domain of complex networked culture rather than as merely passive resistance under the surveillance of God.

5 The new authenticity and the surveilled self

This active connection between the surveilled self and the revelation of an authentic lifestyle or real self can be seen at play in a variety of both religious and secular discourses.

Mark Andrejevic (2002; 2003) has argued that the current bonanza in reality TV programming has helped “to define a particular form of subjectivity consonant with an emerging online economy: one which equates submission to comprehensive surveillance with self-expression and self-knowledge” (2002:253) rather than corporate or governmental control. Reality TV programs have also become in some senses “training” documentaries for what Andrejevic calls lateral surveillance: the call for good citizens to watch one another. In the new televisual economy that Andrejevic describes this willingness to subject oneself to surveillance serves as a demonstration of the strength of one’s self-image.

Being ‘real’ is a proof of honesty, and the persistent gaze of the camera provides one way of guaranteeing that ‘realness’. Further, in a teeming society wherein one’s actions often go unnoticed by others, the reality of those actions can be validated if they are recorded and broadcasted – they become more real to oneself to the extent they become real for others. Submission to comprehensive surveillance is a kind of institutionally ratified individuation: it provides the guarantee of the authenticity of one’s individuality. (266)

The sense of not having anything to hide is both reified and problematised by these programs. If everything is in view then both the realness and the manipulative construction of character become evident, as do the prevailing models of normative characterisation.

Surveillance data and a variety of video and audio evidence, are not just used in reality programming they are now essential plot devices in popular crime shows. Here the forensic power of surveillance data is shone on characterisations of the deviant and the criminal. Hardly an episode goes by in series like the *CSI* franchise without someone pouring over hours of CCTV footage from a crime scene. Such

work is often represented as mundane but fruitful, as one amongst many forms of looking at/through evidence. Often however it comes to the forefront of the plot and takes on a more integral element linking the voyeuristic game of viewers and characters. The connections between forensic logic, the apocalyptic and visual surveillance are also evident. Like prophecy believers, television's forensic scientists are looking for the signs of the times, for portents that will help them understand reality and in each of these episodes "reality" or "evidence" is mediated through a series of visual signs.

Recently broadcast episodes⁴ of two popular crime dramas, *CSI* and *Criminal Minds*, bear this out. In an episode of *CSI*,⁵ CCTV footage is used to reconstruct a complex multi-gunman supermarket shoot out. In the following episode of *CSI Miami*⁶ it is not CCTV footage but the video extras from a pornstar victim's most recent film that provides the video evidence. In recent episodes of *Criminal Minds* surveillance footage is even more central. One storyline⁷ is constructed around a paedophile's online video auction of a child through a live web cam feed time-stamped to indicate the minutes and hours left before the child goes to the highest bidder. The next episode⁸ features videos of a sadistic duo who send DVDs to their victims' mothers. In each of these instances the video evidence is read by the protagonists and the viewers as a potential revelation of something real or authentic about the victims or their unknown attackers. The DVDs from the sadists for example, are read closely by the show's behavioural scientists to reveal the presence of the unseen accomplice. In a pop-psychological interpretation – a staple of this show – it is also read as an "intrinsic" element of the two criminals' "perversion." We are told that the accomplices "need" the video evidence as an artefact to share and a way of reliving their sadistic crimes.

The connections between the surveillance data and the apocalyptic moment are particularly acute in the paedophile auction episode of *Criminal Minds*. The "ticking" clock code at the bottom of the live feed, which allows paedophile voyeurs into the world of the child, is a literal marker of the countdown to the apocalyptic fate that awaits the boy when the auction is over. It is also a marker for the work of the criminalists of the FBI, who have a limited time span to decipher the images before them. It thus represents both a fated end and a hoped for salvation.

4 The episodes of *CSI* and *Criminal Minds* were broadcast in Australia on 29 and 30 July. As Nick Groombridge (2002) points out in his survey of CCTV imagery on popular television this method of looking to episodes "at hand" may seem random but is indicative of the widespread references in popular culture because almost any night or week's viewing can be chosen and will yield interesting "results" for analysis. While the episodes discussed here were broadcast over two days recently in Australia they include repeats that had first aired in the United States in 2004. They thus represent a narrative of surveillance that has remained "current" over the last three years.

5 "Paper or Plastic" Episode 83/Season 4 first broadcast 12/02/2004

6 "Innocent" Episode 48/Season 2 first broadcast 24/05/2004

7 "P911" Episode 24/Season 2 first broadcast 27/09/2006

8 "The Perfect Storm" Episode 25/Season 2 first broadcast 04/10/2006

The time codes of surveillance footage marks it as a mediation of both “real” bodies and of “real” time and in shows like *CSI* and *Criminal Minds* it is the ability to read the complex evidence of space and time together that is often most revealing. This work is imaginative and psychological, it involves the players getting “inside” the heads of the criminals or reconstructing the crime after the event. It is often through staring at these surveillance images that insight occurs – in a pseudo-visionary experience – allowing a connection to be made between the after image and the real bodies of the crime.

6 The forensic and the apocalyptic body

Novelist J. G. Ballard has written of his own fascination with the *CSI* series and asks the question: “Why is it so riveting?”. He finds his answer in an existential apocalypticism: the finality of the autopsy room, which he describes as the “inner sanctum” of the series:

Here the victims surrender all that is left of their unique identities, revealing the wounds and medical anomalies that led to their demise. Once they have been dissected – their ribcages opened like suitcases, brains lifted from their craniums, tissues analysed into their basic components – they have nothing left, not even the faintest claim on existence. I suspect that the cadavers waiting their turn on the tables are surrogates for ourselves, the viewers. The real crime the C.S.I. team is investigating, weighing every tear, every drop of blood, every smear of semen, is the crime of being alive. I fear that we watch, entranced, because we feel an almost holy pity for ourselves and the oblivion patiently waiting for us. (Ballard 2005)

But Andres Vaccari (2005) accuses Ballard of missing the point: yes the body on the table is key but the fantasy of *CSI* is not just psychological, there is also “a right-wing edge to *CSI*, a morally conservative paranoia”:

CSI is, in fact, a parable about the War on Terror. It is full of paranoid warnings, admonitions, explorations of fear. The space the forensic investigators tread on every day is a landscape of death and remains, of accidents and rotten intentions. This is the modern traumascap, an unsafe and paranoid place, a netherworld of catastrophe and loss. No, there’s no heaven; just decomposing bodies, flesh cracked open on the stainless-steel table, organic fluids and chunks of tissue under the microscope. *CSI* portrays a world in which we have come to accept these things as necessary and inevitable.

Investigating this televisual traumascap requires what Rugoff (1997) has dubbed “forensic aesthetics.” He notes (1997:91) that “any good investigator...must have a nose...for smelling out the significance not only of seemingly trivial clues but of non-events and missing details as well.” It is the overall “gestalt” of the “crime scene” that matters because “clues do not betray their secrets when directly examined;

their story emerges only if they are approached obliquely.” This forensic aesthetic finds surprising resonance in the Christian apocalyptic. Rugoff’s “gestalt” echoes VonRad’s (1975) apocalyptic “cipher” described earlier. For prophecy believers the world is in fact a “crime scene,” an “after image” that follows on from the original sin of Adam and Eve (Genesis 3). And both the Christian apocalyptic and Rugoff’s forensic aesthetic are corporeal narratives that depend on the trace of the body for their impact and intrigue. The aftermath of the expulsion from Eden is always a bodily experience, more specifically of the body under surveillance. Expelled from the garden Adam’s first thought is of his body, a new instinct, a sensation of being watched, compels him to cover his nakedness, and quickly following this experience of bodily shame comes the realisation of bodily exertion: he will have to labour to feed and clothe the body.

As Ballard notes, in the inner sanctum of forensic dramas is the autopsy table, on the autopsy table the contemporary body is naked but not in a pre-edenic sense, here the apocalyptic signs of pain, exertion and violence are examined. The *Book of Revelation* might be read as a bizarre autopsy report of “the lamb that was slain” (Rev 5:6; 13:8) so crucial is the wounded body in this narrative. Christian commentators like to point out that it is “the lamb that was slain” who is triumphant in *Revelation*. (cf Barr 1984). Many argue that this is a remarkable image of a reverse theology of power: the weak will come to rule over the brutalising and the strong. However what is perhaps more notable is that the lamb is not the only figure in *Revelation* who is slain. The book is awash with ruptured bodies. As Elana Gomel (2000) has pointed out, *Revelation*’s “baroque scenarios are shaped by the eroticism of disaster” and these erotics are double edged:

On the one hand, its ultimate object is some version of the crystalline New Jerusalem, an image of purity so absolute that it denies the organic messiness of life. On the other hand, apocalyptic fictions typically linger on pain and suffering. The end result of apocalyptic purification often seems of less importance than the narrative pleasure derived from the bizarre and opulent tribulations of the bodies being burnt by fire and brimstone, tormented by scorpion stings, trodden like grapes in the winepress. In this interplay between the incorporeal purity of the ends and the violent corporeality of the means the apocalyptic body is born. (Gomel 2000:405)

In the current environment the image of the devastated apocalyptic body – the bodies still falling from the towers of September 11, the bodies of Abu Ghraib, the bodies of starvation in Darfur – seem to elide any millennial hope. The forensic analysis of such images refuses to give up its meaning and leaves us hankering for a conjuring trick that will transform the vulnerability they do reveal.

These connections between apocalyptic bodies and the contemporary security state become acute in the world of nanotechnologies. These evolving technologies produce the mechanisms whereby human bodies become controllable nodes in

an information network of somantic surveillance. “Smart-warriors” become fully mission-controlled through an array of wearable and implantable technologies that see, sense and report. It is here that the discourse of future bodies oversteps the messiness of today’s realities. Monahan and Wall (2007) point out that these technologies are caught between current realities and a discourse about their future potential. They note that this discursive “history of the future,” also creates the necessary parameters for generous funding and development opportunities.

Discourses about the revolutionary potential of nanotech should also be read as cultural tools for conjuring those worlds into existence, while simultaneously foreclosing alternative pathways for technoscientific development.... By stressing the “new” groundbreaking features of nanoscience and nanotechnology... proponents of nanotech biomedical monitoring seek to construct a “break in time”.... or a point at which the future lifts off from the present, transporting us away from current problems and concerns. In this framing, any resistance to such bold futures is seen as increasing national vulnerability to terrorists who might not be as ethically constrained or responsible as the US. (Monihan & Wall 2007:159)

While these “bold futures” are being explored for very real military and corporate ends, in a fascinating feedback loop this discourse of the future has also found its way back into contemporary reimaginings of traditional apocalyptic bodies such as the Beast micro-chip of the *Left Behind* novels.

7 The image rhetorics of surveillance and national security

Films, television drama and popular cultural artefacts like *Left Behind* are critical players in the contemporary “image rhetorics” of securitisation (Muller 2004). We live in an environment where security – national, homeland, personal – must be configured in response to what Liotta (2005) calls “creeping vulnerabilities” as well as specific “threats”. And as Barkun notes it is also an environment in which “war” and “disaster” are conflated with very real policy consequences:

It implies that all forms of emergency response must be linked, whether civilian or military, national or local. This potential breaching of boundaries between types of response mirrors the breaching of conventional boundaries among types of threats. Thus there are no longer clear distinctions between war and peace, war and crime, war and disaster. Rather myriad forms of “low intensity” conflict inhabit a transnational zone of ambiguous events (Barkun 2002:31)

This “transnational zone of ambiguous events” is not just apparent in the news and the rhetoric of politicians. As we have seen the “traumascape” of popular crime shows and the apocalyptic scenarios of prophecy novels all contribute to this ongoing sense of low intensity conflict and creeping vulnerabilities. Popular culture is not just used by viewers to try to make individual psychological sense of this contemporary

situation it is also a potent tool available to advocates and policy makers. Popular image rhetorics are an essential part of conjuring the history of the future. Benjamin Muller argues, for example that “by exposing the painful procedures necessary for cheating biometrics, films like *Minority Report* only strengthen the resolve to introduce such technologies into the contemporary politics of discriminating friend from foe.” He continues:

Minority Report, *Mission Impossible*, and other films, become the space in which the merits, dilemmas, and even considerations of political agency are evaluated. In this sense, it would seem that industry representatives and policy advocates consistently evoke Hollywood representations of biometric technologies in order to justify the introduction of such measures and even extol their virtues. (Muller 2004:286)

Michael Shapiro gives quite a different reading of this same situation. In his formulation, the hero’s painful eye surgery to avoid retinal identification is a decisive movement that marks John Anderton (the Tom Cruise character) as a “subversive body”.

He manifests a counter energy and goes so far as to modify his body to subvert the surveillance system...Anderton is therefore a Deleuzian fugitive; “Everybody runs,” he says when the police first try to apprehend him, and thereafter his running requires him to move in ways that allow him to escape from the coding apparatuses and exemplify the Deleuzian suggestion that there are always forms of flow that elude the capturing, binary organizations. (2005:30)

Significantly, as Shapiro points out, this is a critical movement from the opening scenes of the film where Anderton’s body is choreographed as an integrated part of the surveillance machinery of the state.

Minority Report can and will be read both ways by audiences, critics and policy makers. And certainly overall the discourse of “the history of the future” is inherently unstable and competing fragments will ensure that is not reduced to either unadorned paranoia or easy optimism. However there is no doubt that since September 11 there does seem to have been a shift in the way that surveillance futures are conceptualized and represented. As the *Time* magazine article quoted at the beginning of this paper and much of the press coverage of the July 2007 London bombings indicates, the balance between surveillance as protection and surveillance as intrusion has tilted dramatically. As one commentator put it recently: “I think the genie is out of the bottle.” Paul Levinson, chairman of communication and media studies at Fordham University told the *Washington Post* that people now have different expectations about their right to privacy. And the genie that has escaped?

“The genie is the lowest level of privacy that human beings have had in their history,” Levinson says. “We just have to get used to it. It’s a question of redefining what our public and private lives are.” (Duke 2007)

One recent media survey (Lirtzman 2007) indicates that 70% of Americans

support the increased use of surveillance cameras in public places and another shows 62% support continued wiretapping to fight terrorism (Duke 2007). *Post* writer Lynne Duke identifies Jason Bourne and Jack Bauer⁹ as part of a culture that promotes a new “swashbuckling and romantic” view of surveillance.

In these types of adrenaline-pumping portrayals of electronic eavesdropping, reality must step aside so that Bourne (when he’s not crashing a car) or “24’s” Jack Bauer (when he’s not torturing someone) can eavesdrop in real time, real fast. And it’s always for the good, you see, because Bourne’s gotta find out what sinister spook programmed him to be a stone-cold killer and Bauer’s gotta save the world. The ends justify the means. No time for questions. (Duke 2007)

Certainly cries of “I’m repositioning the satellite now” or “Send the feed to my PDA” are part of the familiar patter that pretends to make shows like *24* “realistic” encounters with contemporary technologies of spying. Nicola Rafter has detected a similar “swashbuckling” attitude in another recent surveillance film: Tony Scott’s *Deja Vu*. Although it has the structural earmarks of classic surveillance films it bears little of the social critique. It uses a futuristic surveillance device as a principle visual element but does not use it as a plot device to critique technology or to explore the character’s identity. (Rafter 2007)

But not all recent surveillance films take this approach. *The Lives of Others* has enjoyed both critical acclaim – an Oscar for Best Foreign picture – and unusually long playing seasons at Melbourne and Sydney arthouse cinemas. At its heart is a devastating critique of the East German surveillance state under the Stasi. Although the brutality of the state is represented through the ubiquity of its surveillance, the intensity of its interrogation techniques and the corruption of friend against friend that this inculcated, the film also presents a story of resistance and transformation. This attempt to produce a transformational story has been criticised by those who believe it fails to come to terms with the severity of the East German security state (Ash 2007; Funder 2007).

What is unique about Florian Henckel Von Donnersmarck’s debut feature and what troubles his critics from the point of view of history, is the portrayal of a genuine “encounter” through the mechanics of surveillance. Stasi agent Gerd Wiesler is gradually transformed through his day-to-day encounter with playwright Georg Dreyman and his circle of friends who have been placed under surveillance. Wiesler gradually becomes addicted to their lives as he sits in the attic of Dreyman’s apartment building listening to the clumsy old reel-to-reel wire taps. His existential encounter with the lives of others leads to his taking unusual risks to protect them. Whether such risk taking would have been historically possible given the multiple levels of lateral surveillance in place during the Stasi era is not my concern here.

9 Jason Bourne is the lead character played by Matt Damon of three highly successful movies (*The Bourne Identity*; *The Bourne Supremacy*; *The Bourne Ultimatum*) about a rouge CIA assassin. Counter terrorism agent Jack Bauer, played by Kiefer Sutherland is the hero of six seasons of the high-rating television drama *24*.

What I find interesting is the way this narrative, this reimagining of the past, links in with contemporary narratives of surveillance as a site of authenticity. While, as we have seen, the culture of reality TV “equates submission to comprehensive surveillance with self-expression and self-knowledge,” (Andrejevic 2002:253) Von Donnersmarck’s film explores this relationship from the other side. Surveillance becomes not an objectifying method of control – of “othering” – but a site of existential encounter *with* the other. Both self and other are reimagined in this encounter.

8 Conclusion

The trope of surveillance is ubiquitous in contemporary culture and the reach of surveillance technology in contemporary urban spaces is constantly expanding through both technical advances and policy creep. Two metaphors have commonly been adopted to mediate reflections on cultures of surveillance. At a popular level the Orwellian figure of Big Brother has been the focal point for fears of technological encroachment on private lives. At a policy or academic level the Foucaultian Panopticon¹⁰ (Foucault 1977) has often been employed to conceptualise the modern disciplinary power of the surveillance state.

I have argued in this paper that the discourse of the apocalyptic and the forensic are deeply embroiled in contemporary cultural mediations of surveillance. These narratives allow for both a critique of surveillance cultures as well as an interrogation of unexpected resistances, opportunities, fears and new cultural spaces of the surveilled subject.

Neither of these narratives allow us to abandon the totalitarian metaphors of Big Brother and the Panopticon. As Maier (1997) notes the apocalyptic omniobservant God is a model of Foucault’s panoptic watcher. But the twin impulses of the apocalyptic and the forensic: transformation and catastrophe; discovery and horror; enable us to conceptualise the cultural work of surveillance in a range of ways. One of the surprising insights that emerges at the intersection of these narratives is a story of authenticity and self discovery that shadows the wider story of state intervention that subjects identity to interrogation in quite different ways.

As media academic Paul Levinson said to the *Washington Post*: “the genie is out of the bottle.” He might have added: be careful what you wish for.

References

- Andrejevic, Mark, 2002, “The kinder, gentler gaze of Big Brother: Reality TV in the era of digital capitalism,” *New Media Society* 4 (2) pp. 251–270
- Andrejevic, Mark, 2004, *Reality TV: the work of being watched*, Rowman & Littlefield, Lanham, Md.

¹⁰ This model prison has been widely described, with its unseen watcher in the middle and its prisoners constantly on view around the perimeter. The *possibility* of surveillance at any point becomes the disciplining factor leading to extremely effective internalised self-surveillance.

- Ahearn, Edward J., 1996, *Visionary fictions: apocalyptic writing from Blake to the modern age*, New Haven: Yale University Press.
- Ash, Timothy Garton, 2007, "The Stasi on Our Minds," *New York Review of Books*, Volume 54, Number 9 · May 31.
- Ballard, J., G., 2005, "In Cold Blood," *The Guardian*, June 25, available online: <<http://film.guardian.co.uk/features/featurepages/0,,1512152,00.html>> accessed: 28 July 2007.
- Barkun, M., 2002, "Defending against the apocalypse: the limits of homeland security," *Policy Options*, September 2002, pp. 27-32
- Barr, D.L. 1984, 'The Apocalypse as a Symbolic Transformation of the World: A Literary Analysis', *Interpretation*, vol. 38, no. 1, pp. 39-50.
- Boyer, P.S., 1992, *When time shall be no more: prophecy belief in modern American culture*, Belknap Press of Harvard University Press, Cambridge, Mass.
- Cohn, Norman, 1970, *The pursuit of the Millennium: revolutionary millenarians and mystical anarchists of the Middle Ages*, Revised and expanded edn, Maurice Temple Smith Ltd., London,.
- Dellamora, R., 1995, *Postmodern apocalypse: theory and cultural practice at the end*, University of Pennsylvania Press, Philadelphia.
- Dixon, Wheeler W., 2003, *Visions of the Apocalypse: spectacles of destruction in American cinema*, London; New York: Wallflower.
- Domke, D.S. 2004, *God willing?: political fundamentalism in the White House, the "War on Terror," and the echoing press*, Pluto Press, London
- Duke, Lynne, 2007, "Who's on the Line? These Days, It Could Be Everyone," *Washington Post*, August 12; Page D01, available online: <<http://www.washingtonpost.com/wp-dyn/content/article/2007/08/11/AR2007081101219.html>> accessed 12 August 2007
- Foucault, Michel, 1977, *Discipline and punish: the birth of the prison*, London: Allen Lane.
- Frykholm, A.J. 2004, *Rapture culture: left behind in Evangelical America*, Oxford University Press, Oxford, England; New York.
- Funder, Anna, 2007, "Eyes without a Face," *Sight and Sound*, May.
- Gomel, Elana, 2000, "The Plague of Utopias: Pestilence and the Apocalyptic Body," *Twentieth Century Literature*, Vol. 46, No. 4, pp. 405-433
- Gorenberg, G., 2000, *The end of days: fundamentalism and the struggle for the Temple Mount*, Free Press, New York.
- Gates, David, 2004, "The Pop Prophets," *Newsweek*, May 24, available online: <<http://www.msnbc.msn.com/id/4988269/site/newsweek/>> accessed 25/07/07.
- Groombridge, Nic, 2002, "Crime Control or Crime Culture TV?" *Surveillance & Society* 1(1): 30-46
- Hultgard, A. 1998, 'Persian apocalypticism', in J.J. Collins (ed.), *The encyclopedia of apocalypticism, Volume 1: The origins of apocalypticism in Judaism and Christianity*,

- Continuum, New York, pp. 39-83.
- Juergensmeyer, M., 2003, *Terror in the mind of God: the global rise of religious violence*, 3rd edn, University of California Press, Berkeley.
- Kermode, F., 2000, *The sense of an ending: studies in the theory of fiction: with a new epilogue*, Oxford University Press, Oxford; New York.
- Lirtzman, Michelle, 2007, "Surveillance Cameras Win Broad Support" ABC News, July 29, available on line: <<http://www.abcnews.go.com/US/story?id=3422372&page=1>> accessed 3 August 2007
- Liotta, P.H., 2005, "Creeping Vulnerabilities and the Reordering of Security," *Security Dialogue*, Vol. 36 No. 1, pp.49-70
- McMinn, Lisa, 2001, "Y2K, The Apocalypse, and Evangelical Christianity: The Role of Eschatological Belief in Church Responses" *Sociology of Religion*, Vol. 62, No. 2, pp. 205-220
- Maier, H. 1997, "Staging the Gaze: Early Christian Apocalypses and Narrative Self-Representation", *The Harvard Theological Review*, vol. 90, no. 2, pp. 131-154.
- Maxwell, Richard, 2005, "Surveillance: Work, Myth, and Policy," *Social Text* 83, Vol. 23, No. 2
- Monahan, Torin and Tyler Wall, 2006, "Somatic Surveillance: Corporeal Control through Information Networks," *Surveillance & Society*, 4(3): 154-173
- Muller, Benjamin J., 2004, '(Dis)qualified bodies: securitization, citizenship and 'identity management'', *Citizenship Studies*, 8:3, 279 - 294
- New, D.S., 2002, *Holy war: the rise of militant Christian, Jewish, and Islamic fundamentalism*, McFarland & Co., Jefferson, N.C.
- O'Donnell, M., 2004b, "'Bring it on': the apocalypse of George W. Bush," *Media International Australia Incorporating Culture and Policy*, No 113
- O'Leary, Stephen D., 1994, *Arguing the apocalypse: a theory of millennial rhetoric*, New York: Oxford University Press.
- Pippin, T. 1999, *Apocalyptic bodies: the biblical end of the world in text and image*, Routledge, London; New York.
- Quinby, Lee, 1994, *Anti-Apocalypse: exercises in genealogical criticism*, University of Minnesota Press, Minneapolis.
- Quinby, Lee, 1999, "Women and the Techno-Millennium," *Review of Education, Pedagogy, and Cultural Studies*, 21:4, 281 - 300
- Rafter, Nicola, 2007, "Surveillance and Spying in Film: I – Déjà vu," *OUPBlog*, February 22, available online: <http://blog.oup.com/2007/02/surveillance_an2/> Accessed 16 July 2007
- Ripley, Amanda, 2007, "Can We Spot The Threat?" *Time*, 16 July 2007
- Robbins, Thomas and Susan J. Palmer (eds), 1997, *Millennium, messiahs, and mayhem: contemporary apocalyptic movements* New York: Routledge.
- Rowley, David G., 1999, "'Redeemer Empire': Russian Millenarianism' *The American Historical Review*, Vol. 104, No. 5 pp. 1582-1602

- Rusconi, R., 1998, "Antichrist and Antichrists" in Bernard McGinn, *The encyclopedia of apocalypticism volume 2: Apocalypticism in Western history and culture*, New York; London: Continuum, pp287-325
- Schaefer, N. A., 2004, "Y2K as an Endtime Sign: Apocalypticism in America at the fin-de-millennium," *Journal Of Popular Culture* Vol 38; Number 1, pp 82-105
- Schüssler Fiorenza, E., 1998, *The book of Revelation: justice and judgment*, Fortress Press, Minneapolis.
- Schüssler Fiorenza, E. 1991, *Revelation: vision of a just world*, Fortress Press, Minneapolis.
- Sharrett, Christopher, 1993, *Crisis cinema: the apocalyptic idea in postmodern narrative film*, Washington, D.C.: Maisonneuve Press.
- Shuck, G.W., 2004, "Marks of the Beast: The *Left Behind* Novels, Identity, and the Internalization of Evil," *Nova Religio: The Journal of Alternative and Emergent Religions*, Vol 8, No 2, pp. 48-63.
- Shuck, G.W., 2005, *Marks of the beast: the left behind novels and the struggle for evangelical identity*, New York University Press, New York.
- Tapia, A. H., 2002, "Techno-Armageddon: The Millennial Christian Response to Y2K," *Review of Religious Research*, Vol. 43, No. 3, pp. 266-286
- Vaccari, Andres, 2005, "Why I love/hate CSI," available online: <<http://andresvaccari.com/blog/?p=23>> accessed: 28 July 2007
- Van Melik, Rianne, Van Aalst, Irina and Van Weesep, Jan
- Webb, R.L. 1990, "Apocalyptic': Observations on a Slippery Term', *Journal of Near Eastern Studies*, vol. 49, no. 2, pp. 115-126.
- West, M. & Carey, C. 2006, '(Re)Enacting Frontier Justice: The Bush Administration's Tactical Narration of the Old West Fantasy after September 11', *Quarterly Journal of Speech*, vol. 92, no. 4, pp. 379 - 412.

15

Auto-ID and location-based services in national security: Social implications

Holly Tootell

Lecturer, School of Information Systems and Technology, University of Wollongong

Abstract

This paper provides an overview of auto-ID and location-based service technologies that are currently being used for the purposes of national security. The paper addresses the social dimensions of technology which have a bearing on their acceptance by individuals. This overview from both a technology and social perspective allows for an understanding to be created as increasingly decisions regarding adoption need to be made by different sectors in society.

Keywords: automatic identification, location-based services, national security, terrorism, liberty, privacy, security

1 Introduction

The primary purpose of a literature review is to provide evidence of relevant research being conducted in a particular field of study. This paper explores the use of auto-ID and location-based services technologies for national security purposes. This includes discussion of technologies currently being used, and also discussion of technologies being proposed for national security applications. Firstly the development and role of location technologies is covered in regard to national security. Secondly, a critical review of the social constructs that relate to the introduction of the technologies is necessary. This issue is addressed through the social dimensions of the technology, sometimes thought to be the consequences of its use: privacy and security. These concepts need to be treated separately but are closely related. Thirdly, the current context of national security and technology will be examined.

2 Background to automatic identification and location-based services

The following sections provide a review of auto-ID and LBS technologies. Each section begins with an overview of the technology and then moves to examine their presence in the national security arena. The sections have been organised in line with the historical development of the technology. This progression reflects an increase in precision of location identification.

Auto-ID technologies are those capable of providing automatic identification where human intervention is not required (Ames 1990a, b, c; Cohen 1994; Michael et al. 2006b). Auto-ID has traditionally been equivalent with barcodes, used on goods in stores and cards for financial transactions. The scope of use is now more widespread, with uses ranging from immigration control systems to pet identification. Auto-ID technologies have had a mass market presence since the 1960s and their potential for detrimental impact on human rights and privacy have been noted since the 1970s (Michael and Michael 2004, p.434).

The following technologies have been developed over the past 50 years. The drivers for this technology development have been the move by governments to adopt electronic systems to replace the use of paper-based methods (such as vouchers, coupons, ration cards and concession cards) to operate large-scale federal and state programs, in order to increase efficiency (Michael and Michael 2006a, p.21). Other reasons include greater social acceptance and affordability of the technology. Each of the following technologies has made a significant contribution to the area of location-based services, however it is their convergence that is of interest as discussion moves toward the role of location-based technologies in relation to national security. Smart cards, biometrics, RFID, GPS and GIS are technologies that alone or in combination provide information about the location of a user. Biometric technologies do not track location directly, but biometric identification

on a smart card ensures that every time the smart card is used to access a building for example, a time and date stamp of that biometric identification and smart card access is logged. This is able to be pieced together to enable movement patterns to be established. GPS on the other hand is a real-time location tracker.

This research is concerned with the issue of the automatic identification of people through location determination for national security purposes, in order to understand whether a trade-off is made for enhanced perception of security, or sacrificed in order to maintain an illusion of security.

2.1 Smart cards

A smart card is a credit card-sized plastic card that consists of an integrated circuit or 'chip' which enables the card the ability to store and/or process data. There are two broad categories of smart cards: memory cards that contain only non-volatile memory storage components, and perhaps some specific security logic; and microprocessor cards that contain memory and microprocessor components.

Smart cards emerged from the development of magnetic strip cards. The innovation of the smart card was devised by Juergen Dethloff of Germany. The first patent, although restricted to Japan, was taken out by Arimura in 1970. The first international patent was given to Frenchman Roland Moreno in 1974, who founded the Société Internationale pour l'Innovation. This society was established to develop new technologies and extend its patents world wide (Rankl and Effing 2000; Zoreda and Oton 1994).

Smart cards have been adopted by many industry sectors for a variety of purposes. Table 1 provides an overview of some of the most common applications (Chaum 2000). In addition to these examples, smart cards are commonly used as access cards to secure areas, as identification cards and as loyalty cards for many different sectors.

Table 1: Smart Card Applications

Industry	Application
Financial	Electronic Purse, Credit/Debit cards and Secure Electronic payments
Transport	Electronic Toll collection, public transport fares and Drivers Licence
Communication	Mobile Phone accounts and Access to Pay TV
Healthcare	Medical Information cards and Government health insurance eligibility
Education	Identification, library access, security access
Government	Non-repudiation device for voting and Government benefit payments
	National Identification schemes
Retail	Discount/VIP/membership cards

The technological development of smart cards has advanced the cards to include larger memory and processing capacity which has increased the functional potential for their application. In line with this is a perceived increase in the threat posed by multi-purpose smart cards in terms of centralisation of data storage. This concern is

addressed specifically in regard to smart card national identification schemes by:
...the simple logic that the higher an ID cards value, the more it will be used. The more an ID card is used, the greater the value placed on it, and consequently, the higher is its value to criminal elements (LSE 2005, p.35).

2.2 Biometrics

Biometrics, as a form of identification, have been in use since early fourteenth century China (Chirillo and Scott 2003, p.2). The earliest recorded uses of biometric identification include Babylonian kings who used handprints to identify different things such as engravings as their own (Harris and Yen 2002); and Chinese merchants in the fourteenth century stamping children's palm prints and footprints on paper with ink to be able to distinguish between them (Chirillo and Scott 2003).

A biometric is a "measurable physiological and/or behavioural trait that can be captured and subsequently compared with another instance at the time of verification" (Ashbourn 1994). It refers to identifying a person based on his or her distinguishing physiological and/or behavioural characteristics (Jain et al. 2000). Biometric identifiers include digital fingerprints, retinal scans, hand geometry, facial characteristics, and vocal patterns.

The public perception of a biometric identification technology is an important component in the success and adoption of a technique. In addition to this, the technique must be legally and physically robust, safe to use, and not invade the user's privacy. An example of this is a fingerprint scanner, which is often associated with criminal identification. The self-protection reflex of the eyes means that many people are uncomfortable with having laser scans on a regular basis and are often fearful of unfounded claims that regular scanning could be detrimental to their health. To contrast this, hand geometry scanning and signature verification are mostly regarded as innocuous (Kim 1995). One of the mistakes often made in the discussions of biometrics and use of parts of the body for identification is where the act of identification can be associated with a violation of bodily integrity (van der Ploeg 1999). Overcoming public perception of the invasiveness of the scan or acquisition of the biometric sample is the key to success of more pervasive use of these technologies.

From the perspective of civil libertarians, biometric identification has been seen as a threat to the location privacy of individuals (Davies 1998; Johnson 2004). However the counter argument recognises that many of the biometric identifiers being requested of a person are things that they have on show most of the time. There is nothing private about your face (Branscomb 1994; Scheeres 2005). The same was said of voice and handwriting by the US Supreme Court. A person's reasonable expectation of privacy could not extend to "those physical characteristics that are constantly exposed to the public" (Woodward Jr 1997, 2001). However, this does not overcome the controversy related to the legal issues surrounding the storage

and usage of biometric identification (Chandra and Calderon 2005; van der Ploeg 1999).

Biometric identification can be used for many purposes. Table 2 groups the uses into three broad categories; forensic, civilian and commercial, and describes typical uses for these forms of identification (Jain et al. 2000; Petersen 2001; Rood and Hornak 2003).

Table 2: Applications for Biometric Identification

Forensic	Civilian	Commercial
Criminal investigation	National ID	ATM security
Corpse identification	Driver's license	Credit card security
Parenthood determination	Welfare disbursement	Cellular phone
Prison security	Border crossing	Access control
	Customs and immigration initiatives	Ecommerce/ebanking transactions
	Protecting critical infrastructure	

Biometric identification is extremely useful for restricting access to areas that involve national security, such as military bases or intelligence centres, and for protecting critical civilian infrastructure, such as water supplies and power plants (Rood and Hornak 2003). It must be noted that technology such as this is not a panacea. No technology solution is absolutely foolproof (Michael and Michael 2006b, p.360).

Some biometric identification programs are mandatory, for example criminal investigation and prison security. At present, almost all other programs are voluntary. However, in some of the programs, biometric identification is used to make the service more attractive to users by providing a faster, or more enhanced service, but other forms of identification are still permitted (Alterman 2003). An example of this is the INSPASS (Immigration and Nationalization Service Passenger Accelerated Service System) program in the US. It has been operating since August 1993 as a voluntary system for frequent travellers. It allows passengers to move through immigration more quickly at the cost of a system that has the potential to create a vast amount of international transfer of their personal data (Davies 1996; Kim 1995). This system has grown from 2000 frequent fliers at the outset, to over 100 000 by the year 2000 (Michael and Michael 2006a).

Van der Ploeg (1999) considers the groups targeted for obligatory biometric identification disproportionately include criminals, recipients of welfare, or other benefits, workers, and immigrants. However she classifies an alternate grouping where biometric identification may typify privilege as well. It may include frequent flyers who have been assessed as 'low-risk travellers', are given the privilege to jump the queue and avoid thorough controls; those who have higher access privileges to

secured spaces, parts of IT systems or authorisation of high-risk types of financial transactions.

Biometrics have the potential to enhance our current reliance on documents such as birth certificates, drivers' licences, and passports to establish each person's true identity. In the future, biometric information may be recorded at birth and incorporated in the birth certificate, using the child's DNA as the prime indicator of identity. In such a case, a person's biometric information (which may change with age) may be linked with his DNA (Rood and Hornak 2003).

2.3 Radio frequency identification

Radio Frequency Identification is a technology used for automatic identification. RFID is a generic term for technologies that use radio waves to automatically identify entities; either live or inanimate. The objects are identified by information that may include a unique identifier, or it could be more complex including data such as: manufacturing history, temperature, or age (Kinsella 2003; Legner and Thiesse 2006).

RFID has been referred to as the new barcode (Kelly and Erickson 2005; Want 2004). The advent of barcode technology revolutionised data capture and handling technologies in the retail industry. RFID has advanced data capture and stock handling to a new level. One of the main advantages of RFID is overcoming the reliance of barcodes on line-of-sight data processing. RFID offers more robust and useful scanning options (Alippi and Vanini 2004; Srivastava 2007). Other advantages discussed by Michael et al. (2006b) are that RFID is not limited by its size and is not vulnerable to magnetic fields, or affected by substances such as dirt or paint which may cover the tag.

RFID systems are being used for many item-level tracking applications. The phrase 'internet of things' is being used to describe the potential network of information that could be created by the use of RFID in the following applications (see Table 3) (Alippi and Vanini 2004; Elliot 2003; Floerkemeier and Lampe 2004; Garfinkel et al. 2005; Hsi and Fait 2005; IIE Solutions 2002; Jayakumar and Senthilkumar 2005; Jones et al. 2004; Juels 2006; Smith 2005; Swartz 2004; Want 2004).

Since September 11 the threat of terrorism has ensured that the tracking offered by RFID is a favoured system implemented to alleviate that threat, be it in shipping containers or passport control. Atkinson (2004) observed that prior to September 11 the use of RFID was limited to supply chain security and loss prevention, however in the post-September 11 world, the focus for RFID is ensuring tamper-proof containers due to terrorism concerns. The continued development of RFID technologies is regarded by many to have a significant impact on the way we conduct our day to day life. US Senator Patrick J. Leahy stated that:

RFID has tremendous potential for improving productivity and security, but it will also become one of the touchstone privacy issues of our times (Swartz 2004).

Table 3: Commercial RFID Applications

Application	Commercial Examples
Baggage tracking in airports	For airport baggage identification, RFID has eliminated the need for manual sorting and lifting and is claimed to have enhanced passenger security.
Supply chain management and supply chain theft reduction	The clothing giant, Prada, have their New York dressing rooms fitted with display screens that can identify a smart-tagged garment when it is bought into the room. The display suggests other styles and colours of the garment – even going so far as to show how the garment was worn at a Prada fashion show.
Automobiles	Remote keyless entry.
Animal tracking	Identification and tracking for enhanced livestock management
Highway toll collection	Highway toll collection using RFID has allowed drivers the convenience of driving straight through checkpoints without needing small change.
Passport security	The inclusion of RFID tags in passports and possibly drivers' licenses acts as an 'anti-counterfeiting feature.
Museum exhibits	Enhancing interactivity of displays.
Automatic product tamper detection	Product integrity can be monitored from factory to retail location. It might also help locate the source of activity when tampering is detected.
Harmful agent detection	The use of passive-detector technology could be used on vehicles or security personnel, or in other uses where detection of biological agents are needed.

This sentiment was reflected by Rick Duris, from *frontline Solutions Magazine*, and recorded by Albrecht and McIntyre (Albrecht and McIntyre 2005):

RFID will have a pervasive impact on every aspect of civilization, much the same way the printing press, the industrial revolution and the Internet and personal computers have transformed society...RFID is a big deal. Its impact will be pervasive, personal and profound. It will be the biggest deal since Edison gave us the light bulb.

The pervasiveness in Duris' observation is seconded by Borriello (2005, p.36) who believes that there is an imaginable future where; "Passive RFID tags are in every manufactured object and maybe even in some non-manufactured ones (such as natural resources, animals, and people)."

The US Department of Homeland Security is now using RFID technology at US border checkpoints (Swartz 2004). Visitors entering the US will be issued RFID tags that will track their comings and goings at border crossings. The technology was tested at border crossings in Arizona, New York, and Washington state from the end of July through to spring 2006 (Chabrow 2005). Angell and Kietzmann (2006) puts forward the hypothetical of RFID cash being the preferred method of transaction in the post-September 11 environment, where the threat of anonymity could be removed.

In emergency response situations, like the 2004 Boxing Day Tsunami and 2005 Hurricane Katrina, RFID tags can, and did, assist in management and location

identification of survivors as they were moved between emergency housing facilities or graves (Smith 2005).

Consumer response to RFID is a considerable factor in the future of the technology. Consumer perception is often linked to perceived risks relating to personal data privacy, tracking and remote scanning (Hsi and Fait 2005, p.65; Nath et al. 2006, p.24). Eckfeldt (2005, p.78) puts forward that a clear value proposition to customers is what distinguishes between a successful and shunned RFID application. This is seconded by Ohkubo et al. (2005, p.68), who also raises the problem associated with killing an RFID tag as a privacy protection measure. He suggests that if the tag was 'killed', the consumer would not be able to take advantage of "future emerging services that would rely on the millions of RFID tags likely to be dispersed throughout the consumer environment". A survey by Metro Group, investigating consumer's major privacy fears relating to RFID found that:

Regardless of privacy-enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be (Gunther and Spiekermann 2005, p.74).

2.4 The global positioning system

The Global Positioning System (GPS) is a satellite-based navigation system. It is used by both military and civilian users. GPS allows for precise location determination however accuracy is different for civilian and military applications. The location is determined based on the distance a user is away from the available satellites. The effectiveness and accuracy of GPS can be affected by weather conditions, mountains, buildings and other terrain (El-Rabbany 2002, p.1; Michael and Masters 2006; Oderwald and Boucher 1997, p.2). The most significant drawbacks of the technology for civilian applications are regarded as low availability/coverage in high-rise urban settings, no system integrity and no guarantee of services performance in a shared military/civilian environment (The Royal Academy of Engineering 2004). Getting (1993) believes GPS to be "...the most significant development for safe and efficient navigation and surveillance of air and spacecraft since the introduction of radio navigation 50 years ago".

GPS has been used for over two decades. In that time the range of uses has expanded enormously as the cost of receivers has become less. Areas of applications are outlined in Table 4 (El-Rabbany 2002, p.129-150; ESRI 2007).

Designed primarily as a military tool, GPS is used to facilitate accurate location awareness. This can be applied to command and control of forces and targeting of weapons. Geographical Information Systems (GIS) are systems used to create and manage spatial information. GPS has the ability to identify events that happen in large, hard to monitor areas like borders, harbours or military bases (Friedrick 2003). For security agencies, there is the ability to more accurately manage resources and access privileges once an incident has been identified.

Table 4: Commercial Applications of GPS

Application	Commercial Example
Mapping	Asset management for utility companies and airborne topographic mapping.
Resource Management	Forestry and natural resources: fire prevention, harvesting, aerial spraying.
Farming	Harvest yield monitoring, chemical applications control and property management.
Civil Engineering	Road construction, earth moving and equipment tracking.
Mining	Assistance with drilling, vehicle tracking and surveying.
Surveying	For both land and marine seismic surveying.
Navigation	In-vehicle street directory systems.
Transit	Mass transport: position determination, fleet management and timetabling.
Retail	Delivery fleet monitoring and dispatch assistance.

3 Social dimensions of technology

With regard to technology, security and privacy are often used interchangeably. To ensure privacy of information, security is required; and vice versa, without privacy safeguards in place, security could be compromised. The following sections detail the concepts of privacy and security as they can be experienced by individuals. Other related concepts including surveillance and liberty are also addressed. These concepts are relevant to discussions of the information society, and the power that exists within that framework, which are addressed in the final section. The importance of addressing these aspects in relation to technology is discussed at length by Ellul (1965, p.90), who reminds us that the consequences of a technology are not necessarily of technical significance, but can be of social or organisational consequence.

3.1 Privacy

Privacy is a concept that has eluded a single, clear definition. McLean (1995) likens privacy to the concepts of liberty and freedom: each a concept unable to be easily defined. To define privacy is to limit its scope (Day 1985; Schoeman 1992). Many cultures do not have a single word for the concept the English language knows as 'private' or 'privacy'; this reflects on the complexity of the concept. Day (1985) dedicated an entire thesis to the definition of privacy across cultures and languages and found some five hundred definitions. However, for the purposes of this work, a working understanding is necessary.

Privacy has been recognised as a concept that has evolved with the progress of society, changing to suit the demands of the current times (Gottlieb and Borodin 1973; Rule et al. 1980). Warren and Brandeis (1890) first wrote of the right of privacy in 1890, asserting that privacy was the right to be left alone. Clarke (1997) prefers not to assume privacy is a right: as a right implies an intrinsic and absolute standard,

something not always applicable to privacy. Recognising privacy as an interest that an individual sustains allows for a more flexible definition that suits the application of privacy in both the offline and online environment: a description suited to the purposes of this work.

Privacy and surveillance, although being distinctly separate concepts, continue to be linked together through popular media including fiction and films. This reinforces a perceived public concept of them being one in the same. Popular movies that show this include: *Rear Window* (Hitchcock 1954), *Blowup* (Antonioni 1966), *The Conversation* (Coppola 1974), *The Osterman Weekend* (Peckinpah 1983), *Sneakers* (Robinson 1992), *Lost Highway* (Lynch 1997), *Gattaca* (Niccol 1997), *The End of Violence* (Wenders 1997), *Enemy of the State* (Scott 1998), *The Truman Show* (Weir 1998), *Antitrust* (Howitt 2001), *Panic Room* (Fincher 2002), *Minority Report* (Spielberg 2002), *Collateral* (Mann 2004), *Cache* (Haneke 2005), *The Good Shepherd* (De Niro 2006), *The Departed* (Scorsese 2006) and *Déjà vu* (Washington 2006). In the literary world, George Orwell's *Nineteen Eighty Four* (1949) is an archetypical expression of what life would be like in a totalitarian state where privacy did not exist.

The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment (Orwell 1949).

3.2 Surveillance

Surveillance has been considered to be an important concept over a long period of time; it derives from the French Revolution at the end of the 18th Century. Wigan and Clarke (2006) define three functions for surveillance when it is utilised as a security safeguard: “to anticipate a violation... to detect a violation... or to assist in the identification of the person responsible for a violation or in the authentication of an assertion as to the identity of the culprit”.

In the recent past surveillance has risen to a higher level of interest. This can be attributed to the increase in database systems collecting information about us (Garfinkel 2000) or it can be likened to the concepts of ‘dataveillance’ or ‘panoptic sort’ described by Clarke (1997) and Gandy (1993) accordingly. Both of these terms relate to the ability of collections of information to be equated with power. The increase in technological capability over the past few decades has seen an increase in the potential of machines and systems to collect information and then data mine. The transition to an online economy, or at the very least, online commerce, has created a whole new pool of information to be collected, tracked and stored. Clarke (1997) and Gandy (1993) recognised that collection of data was occurring well before the online world came into existence.

The introduction of online communications, and more particularly electronic commerce, has resulted in a changing attitude to control of privacy. Privacy in the online environment can be considered differently to a 'traditional' notion of privacy. Privacy in the online arena is mostly concerned with the protection of information. The term 'information privacy' has been defined by Clarke (1997) to be an interest held by individuals regarding the control, and handling of data about themselves. Gandy (1993) supports this theme in his notion of 'informational privacy' based on Westin's (Westin 1967) work as the "claim of individuals... to determine for themselves... the extent information about them is communicated to others".

3.3 Data surveillance

Data surveillance, or dataveillance as defined by Clarke (1988), is the:
...systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.

It describes the surveillance practices facilitated by the collection and storage of extensive quantities of personal data. The notion of data surveillance is supported by Flaherty (1989) who classifies the practice of data surveillance within the broader notion of surveillance as the "supervision, observation or oversight of individuals behaviour through the use of personal data" (Davies 1996, p.248). The use of the term data surveillance is quite narrow, however it is very similar to a number of more specific terms outlined below: Langford (2000, p.73) has likened the concept of data surveillance to the practices of data matching, data monitoring and data recording. Bennett (1996) describes the concept of data surveillance as computer matching.

Lyon (2002, p.353) attributes the pervasiveness of data surveillance to the resulting convergence of information technology structures, the Internet and the vast amounts of data which both are able to provide. Barr (1994) believes that the concept of the information society has contributed to the increase in potential of data surveillance. Clarke (1988) believes that the application of information technology has been a factor in the increasing trend towards surveillance technologies and their pervasive use in the surveillance of individuals through the use of personal data. In contrast to these theories based on data surveillance being an entirely new concept, Langford (2000, p.74) believes that the Internet is inextricably linked to and is responsible for the exacerbation of data surveillance techniques and suggests that it has not facilitated, but merely enhanced previously existing techniques.

As Langford (2000) suggests, the concept of surveillance techniques, such as dataveillance, cannot only be attributed to the Internet and other information technology trends, as much contemporary literature tends to suggest. This form of surveillance has been used extensively within paper-based and localised data systems. Subsequently, the Internet and similar trends have not created this new form of surveillance, but merely facilitated the growth of such by utilising existing

techniques by providing access to more information and technology for exploitation (Lyon 2002, p.346). This has been recognised by the Office of the Federal Privacy Commissioner in understanding that the internet has only contributed to the “proliferation of uses of personal information” (OFPC 2006) rather than initiating such dataveillance practices. An extension to the concept of dataveillance has been proposed by M.G. Michael (Michael et al. 2006a): *überveillance*. This term describes a level of surveillance that goes beyond the scope of 24/7 surveillance. M.G. Michael presents the issues for concern as “misinformation, misinterpretation, and information manipulation.”

3.4 Security

Security can be used to describe many different issues but in the context of this research it is about protection (Acharya 2002). The relationship between security and privacy is often blurred, Starner (2001, p.57) distinguishes between them in the following excerpt:

Security involves the protection of information from unauthorized users; privacy is the individual’s right to control the collection and use of personal information.

This is particularly of interest in the context of national security technology innovations such as national ID and terrorism prevention measures (Michael and Michael 2004). Security as a personal pursuit is being free from threat to personal safety. The security in this instance is a perception or ‘feeling’ experienced by an individual which means it is likely to be experienced differently for each person. In terms of the preceding sections and Starner’s (2001) definition given above, security needs to be considered as technology systems that create information are developed. In relation to the auto-ID and location-based technologies focused on in this work, the potential for privacy invasion to occur is high, which is why the need to be aware of security implications is necessary.

A recurrent theme in technology implication discussions is the prospect of a trade-off between privacy and security. Snow (2004, p.156) defines security as a variable dependent on two issues: factors that threaten the things we value and our interpretation of the environment. In this definition, it is clear that security, if placed on a continuum, could have infinite variation depending on personal interpretations of these factors.

4 National security and technology

4.1 National or homeland security

The specific notion of security in relation to protecting a country from threat has been known variously as homeland security and national security. The concept has been linked closely with military developments at points in time, and at others, has referred to a much broader spectrum of protective initiatives designed to

ensure peace is maintained and the stability of government and society. 'Homeland security' has been predominantly found in US-based literature following the events of 11 September 2001. Since then the term has been gaining wider global acceptance. National security is often used interchangeably with homeland security, internal security, border management and counter terrorism (Relyea 2002). In the literature, homeland security is often linked to terrorism. This limits the scope of the discussion, which enables the introduction of the term national security to be a more encompassing phrase to describe the current state of affairs. For the purposes of this thesis national security encompasses the following categorisations as defined by Kun (2004): intelligence gathering and warning; border and transportation security; domestic counter-terrorism; protection of critical infrastructure; defending against outside attacks; and emergency preparedness and response.

The rhetoric since September 11 has focused on the idea of the homeland and the need for it to be protected and kept free from attack. The language of government and media coverage has encouraged the development of the theme of war on terror. This creates bias in the coverage of homeland awareness.

4.2 Sweeping changes in the name of national security

The recent focus on national security has renewed interest in technologies with the potential to be used for security measures. A technology that has experienced this refreshed approach is biometric imaging. Prior to September 11, it was discussed in primarily defensive terms, as public interest focused on the more sinister potential of the technology, and not the improved security potential it could offer. In the immediate period following the attacks, airports announced urgent implementation of scanning programs, and governments undertook expedited reviews of biometrics-based security systems.

The Defense Advanced Research Projects Agency has initiated a project called Human ID at a Distance which aims to "develop biometric technologies... that can be deployed to identify a known terrorist before he closes on his target" (Alterman 2003). The US Department of Defense (DoD) is supporting research into the application of biometrics, establishing the Biometrics Fusion Centre in Bridgeport, West Virginia. The centre is to help evaluate, implement, and integrate biometric technologies for DoD organisations. The US DoD has adopted a smart card (with an embedded chip) as the standard method of identifying its employees and controlling access to its sites. The DoD plans to add biometric information to the card within the next year (Alterman 2003).

The ability of biometric systems to grant authorised users access to privileged information and protected devices, while denying the same access to others, means that they can assist with the protection of military facilities, airports, industrial plants, offices, retail stores, personal residences, and recreational areas. Rood and Hornak (2003) have questioned whether this form of identification and management of person access would have prevented the events of September 11.

4.3 Legislative changes

The events of September 11 were a turning point for legislative changes. Although the US, UK and Australia had counter terror measures in place, many changes were made in the period since September 11 (Goldstone 2005; Northouse 2006). Some of the changes have met with much criticism from civil rights groups as they are seen to stretch the limits of allowable actions.

The United States Congress passed the following Acts which enhanced the reach of biometric identification of citizens and aliens: the PATRIOT Act – several measures to improve the government’s ability to detect foreign threats operating in the United States. Wire taps surveillance and subpoenas; the Aviation and Transport Security Act and Enhanced Border Security and Visa Entry Reform Act

These were privy to an extraordinarily fast track through to becoming legislation which was noted by many civil libertarians. This fast track came in the presence of warnings prior to September 11 that the US Department of Defense did not have concrete plans in place to address emerging threats (Michael and Masters 2006).

The change in this approach has had follow-on effects to other countries. Australia and UK have border control law updates, and more dangerously, it is being used as a ruse to justify other far greater repressive actions (Goldstone 2005, p.165). The technology impact can be seen in the biometric passport system implemented in Indonesia, considered to be the world’s most comprehensive and decentralised (Poessl 2006); the implementation of BioPass in Singapore, which claims to have enhanced security features to prevent tampering (Yeo 2006) and, Thailand has started issuing citizens with a Java-based multi-application smart card, used primarily for security purposes in the initial deployment (Bergman 2005).

5 Social implications of national security

5.1 Liberty

Liberty, as defined in the Oxford Dictionary of Philosophy, is of concern in almost all constitutions. It associates the value of liberty with autonomy, and as dependent upon the nature of the social context rather than on individual rights (“liberty” 1996). Liberty is also understood as

...the right or power to do as one pleases ...right, power, opportunity, permission ...freedom from control by fate or necessity ...a right, privilege, or immunity, enjoyed by prescription or grant ...setting aside of rules or convention (“liberty n.” 2004).

It is this list of expected freedoms that some fear is being threatened in the post-September 11 world. Increasing technology pervasiveness is a threat to being free, or doing as one pleases. At extremes, it is taking away the power of choice. The adoption of auto-ID and location-based technologies in a mandatory scheme will challenge this definition of liberty. There is certainly a need to balance effective law

enforcement initiatives in the threat of terrorism, but commentators are pleading for it to be done with respect for civil liberties (Goldstone 2005; Luban 2005; Northouse 2006).

Liberty is inextricably bound together with the human rights movement which is bringing privacy and security issues to the fore. From the research examined, the concept of liberty encompasses the notion of civil liberties. Civil liberties, although an essential part of our society, are often taken for granted where there is no direct threat. Goldstone (2005, p.159) suggests that when society is free of security threats, civil liberties are rarely in danger, but in times of war there is a real danger of overreacting. His comments are particular to the United States in this work, but hold true in a wider realm. Luban continues this theme, distinguishing between times of danger and peace. He draws the concepts of security and liberty together through an inevitable trade-off.

...and the only important question then becomes where to draw the line. How much liberty should be sacrificed in the name of security (Luban 2005, p.242).

5.2 Paying a price

Throughout the research on existing studies, there is a consistent theme of citizens needing to waive certain liberties or have reduced access to services in order for national security initiatives to be fully implemented. This is particularly noticeable in the privacy-based studies. The concept of this can be summarised as the figurative price that the average citizen is 'paying' for this increased level of national security.

However, the concept goes back much earlier and in consideration of many more issues than the rapid advancement of technologies. Over time, identifying the price that is being paid for advancement is a difficult task, and it is harder still to measure. Winner frames this observation in terms of consumer product developments and makes the comment that:

They have gotten used to having the benefits of technological conveniences without expecting to pay the costs. Of course, if anyone had bothered to notice, it should have been obvious that a price for "progress" was being paid all along. It was often a very subtle price, a barely recognizable price, but a real one nevertheless (Winner 1986, p.171).

In Winner's research it is suggested that when people want something to happen, they will find ways to justify the costs that need to be paid. It seems inevitable in this model that it is only when the changes occurring through the payment of costs have gone too far that people are able to step back to look objectively at the impact those decisions have had on their life. The pervasive impact of technologies on daily life is questioned only when certain boundaries are challenged. Winner (1986, p.50) proposes the following issues as costs that are significant enough to

consider limiting the use or development of a technology:

- Its application threatens public health or safety;
- Its use threatens to exhaust some vital resource;
- It degrades the quality of the environment (air, land, and water);
- It threatens natural species and wilderness areas that ought to be preserved;
- Its application causes social stresses and strains of an exaggerated kind.

Ng-Kruelle et al. (2002) established the concept of 'Price of Convenience' as a means for understanding what a consumer is willing to give up of their privacy in order to gain a factor of convenience. This study examined the use of mobile devices. This research has established a direction in technology studies to look beyond the benefits of the tool itself and instead evaluate the impact it can have on the end user. Ng-Kruelle et al. (2002, p.4) discuss the concept of the "price" in the context of mobile commerce applications and the consumer. The phrase under consideration here is the 'Price of Convenience':

At an individual level, any potential "consumer" must always balance costs (giving up for personal information such as location and driving speed) against benefits (such as navigation support).

Technological determinism holds that technology has the ability to shape our lives. Perusco et al. (2006) put forward that the social setting in which the technology emerges is as important as the technology itself. Winner (1986, p.51) believes this position can be countered when there is a clear form and limits on the idea of what a society should be. In terms of lifeworld, there is a linking of technology acceptance and shaping of social evolution. A society wishing to structure and direct its forward progress must be aware of the implications of technology in terms of costs and benefits. Without this knowledge, there is the presupposed position of the technology driving social change and not vice versa. Winner (1986, p.68) quotes Marcuse for the joining of the concept of freedom to technical progress of the advancement of science. The position he takes is that at present, the structures around the development of technology are not supportive of inclusion of lifeworld response. They are rarely designed as technologies of liberation. Michael and Michael pose the same question of balance in terms of the attempt to make the world safer through the use of surveillance cameras and the equipping of children with tracking devices. The consideration here again is whether privacy and freedom are being sacrificed, but they note that:

...more and more people are willing to pay this price as heinous crimes become common events in a society that should know better (Michael and Michael 2004, p.441).

This society is being shaped through many influences particularly in this era of 'real and present danger' of terrorism and biological, nuclear, chemical and radiological threat. The plea in the article is that these and other implications should be considered

in the development stages of technology innovation, not after they are already in place, unable to be changed easily.

Louie and Eckhartsberg (2006, p.70) dispute that a trade-off takes place or even needs to take place. Using the example of data mining they suggest that there are at least five choices that can be made during the process that make a trade-off unnecessary. The weakness here is that these choices rely on individual reasoning looking beyond the self, to the wider implications. Voluntary codes of practice are put forward as an example where this level of decision making has failed, and their fear is that the same will happen in the context of data mining and invasion of liberties.

Westin (2006, p.19) proposes two models from which governments and the wider public are operating (see Table 5).

Table 5: Westin's Security-First and Liberty-First Models

Security First Position	Liberty First Position
If we do not modify some of our traditional constitutional norms limiting government powers, we will not be able to fight terrorism, function as a reasonably safe society and enjoy our liberties.	If we reduce our liberties by granting the government sweeping and uncontrolled investigative and surveillance powers, we will weaken the constitutional system that has made our nation great.

Westin (2006, p.20) believes there are five factors shaping public views in regard to the security versus liberty dichotomy: perceptions of the current terrorist threat and the likelihood of further attacks; perceptions of how well the government is dealing with the threats thus far and the methods being used; perceptions of how government antiterrorist programs are affecting valued civil liberties; underlying orientations toward general security and liberty issues; and basic orientations on political issues in general – which may be shaped by political philosophy, party identification, and demographic factors.

Luban (2005) builds from this consideration framework to personalise the issue more strongly. He strongly supports the notion that a trade-off is taking place and asks what “you” are willing to sacrifice in order to have “minute increments in security”. Luban believes that if the trade-off question is always asked in terms of personal rights, answers may be significantly different to when the questions remain a vague societal generality. He challenges the use of September 11 as the measuring stick by which trade-off questions should be asked:

...we would be willing to sacrifice a lot of liberty to prevent September 11...what sacrifice of our rights would we be willing to undergo to reduce the already-small probability of another September 11 by a factor of, say, one in ten? (Luban 2005, p.243).

Northhouse (2006, p.5) and Wran (2006) support these notions, prompting us to consider the role of technology in understanding the trade-off concerns, and also

recognising the impact and increasing pervasiveness of government in control of personal information.

6 Conclusion

It was stated at the beginning of this paper that location-based services and auto-ID technologies were being used for national security purposes and that their use has a social impact. By examining the technologies currently being used in the area, and also technologies being proposed for national security applications, it was shown that much of the research is happening in technology silos. There is scant research drawing together the technologies in order to understand the impact they have when used collectively for national security purposes.

This paper also established an understanding of the social dimensions of the technology which can sometimes be regarded as consequences of its use. The impact of these technologies on privacy is often discussed from a negative perspective. Although the concepts of privacy, security and liberty intersect to a degree, their interplay with regard to technology use in for national security purposes has been skewed toward the impact of terrorism. The literature on privacy and technology is dominated by works that focus on a threatening impact. This is contrasted with the security literature which proposes technology to be a fix for security concerns. The concept of liberty is manifold, and in the context of technology and national security is seemingly an emotional and tending toward biased patriotism and it seems that a choice must be made: security before liberty, or liberty before security.

The unguarded acceptance of technology as we move through various phases toward an information society, is a trend that has been inevitable, and yet still sinister. We have reached a point in the development of technologies where it is prudent to sit back and look at the potential impacts of what we are designing. Technology for the sake of technology no longer holds importance for the emerging generation. The integration of automatic-identification with location-aware technology has significant benefits for the national security area. Promotion of a technology without consent from the population may be understandable necessity in times of crisis, but the cloak of national security and the associated imminent danger is wearing thin. Technology alone will not prevent terrorist attacks. What it will do is assist society in managing these events when they do happen. Requiring society to remain on elevated levels of alert, or to be 'alert but not alarmed', propagates fear and insecurity. This serves a purpose if the theatre of security can be boosted by the adoption of a technology, however, without democratic debate; this method of technology adoption does little to liberate populations (Brzezinski 2004, p.243).

References

- Acharya, A. 2002, 'State-Society Relations: Reordering Asia and the World After September 11', in K. Booth and T. Dunne (eds), *World in Collision: Terror and the Future of Global Order*, Palgrave, London.

- Albrecht, K. & McIntyre, L. 2005, *Spychips: how major corporations and government plan to track your every move with RFID*, Nelson Current, Nashville.
- Alippi, C. & Vanini, G. 2004, 'A genetic-based application oriented approach to optimize RFID-like passive sensor devices for homeland security', in *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety*, Venice, Italy, 21-22 July 2004
- Alterman, A. 2003, 'A piece of yourself': Ethical issues in biometric identification', *Ethics and Information Technology*, vol.5, no.3, p.139.
- Ames, R. 1990a, 'Opportunities and Challenges', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.6.1-6.11.
- Ames, R. 1990b, 'RF Prophecy', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.5.2-5.6.
- Ames, R. 1990c, 'RF/ID systems', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.3.1-3.9.
- Angell, I. & Kietzmann, J. 2006, 'RFID and the end of cash?' *Communications of the ACM*, vol.49, no.12, pp.91-96.
- Antonioni, M. (1966). Blowup.
- Ashbourn, J. 1994, 'Emerging technology for security and control', *Sensor Review*, vol.14, no.4, p.3.
- Atkinson, W. 2004, 'Tagged: the risks and rewards of RFID technology', *Risk Management*, vol.51, no.7, p.12.
- Barr, T. 1994, 'Australia's information society: clever enough?' in R. Guinery and L. Green (eds), *Framing technology : society, choice and change*, Allen & Unwin, St Leonards.
- Bennett, C.J. 1996, 'The public surveillance of personal data: a cross-national analysis', in D. Lyon and E. Zureik (eds), *Computers, Surveillance and Privacy*, University of Minnesota Press, Minneapolis.
- Bergman, C. 2005, 'Thai smart ID card ready to roll', *Biometric Technology Today*, vol.13, no.5, pp.1-2.
- Borriello, G. 2005, 'RFID: Tagging the world', *Communications of the ACM*, vol.48, no.9, pp.34-37.
- Branscomb, A.W. 1994, *Who owns information?: from privacy to public access*, BasicBooks, New York.
- Brzezinski, M. 2004, *Fortress America: On the Front Lines of Homeland Security, An Inside Look at the Coming Surveillance State*, Bantam Books, New York.
- Chabrow, E. 2005, 'Homeland security to test RFID tags at U.S. borders', *InformationWeek*.
- Chandra, A. & Calderon, T. 2005, 'Challenges and constraints to the diffusion of biometrics in information systems', *Communications of the ACM*, vol.48,

- no.12, pp.101-106.
- Chaum, D. 2000, *Smartcard 2000*, Elsevier Science Publishers, Amsterdam.
- Chirillo, J. & Scott, B. 2003, *Implementing Biometric Security*, Wiley Publishing Inc., Indianapolis, Indiana.
- Clarke, R. 1988, 'Information technology and dataveillance', *Communications of the ACM*, vol.31, no.5, pp.498-512.
- Clarke, R. 1997, *Introduction to dataveillance and information privacy, and definitions of terms*, accessed 2 June 2006, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro>
- Cohen, J. 1994, *Automatic Identification and Data Collection Systems*, McGraw-Hill, London.
- Coppola, F.F. (1974). *The Conversation*.
- Davies, S. 1996, *Monitor*, Pan, Sydney, NSW.
- Davies, S. 1998, 'Biometrics: A Civil Liberties and Privacy Perspective', *Information Security Technical Report*, vol.3, no.1, pp.90-94.
- Day, K. (1985). *Perspectives on Privacy: a Sociological Analysis*. Edinburgh, University of Edinburgh.
- De Niro, R. (2006). *The Good Shepherd*.
- Eckfeldt, B. 2005, 'What does RFID do for the consumer?' *Communications of the ACM*, vol.48, no.9, pp.77-79.
- El-Rabbany, A. 2002, *Introduction to GPS: the global positioning system*, Artech House, Inc., Boston.
- Elliot, M. 2003, 'They had me at Prada', *Industrial Engineer*, vol.35, no.11, p.6.
- Ellul, J. 1965, *The Technological Society*, Johnathan Cape, London.
- ESRI. 2007, *Case Studies*, accessed 2 June 2007, <http://www.esri.com/showcase/case-studies/index.html>
- Fincher, D. (2002). *Panic Room*.
- Flaherty, D.H. 1989, *Protecting privacy in surveillance societies : the Federal Republic of Germany, Sweden, France, Canada, and the United States*, University of North Carolina Press, Chapel Hill.
- Floerkemeier, C. & Lampe, M. 2004, 'Issues with RFID usage in ubiquitous computing applications', *Pervasive Computing*, Springer Berlin / Heidelberg, pp.188-193.
- Friedrick, J. 2003, 'Homeland Security initiatives should boost the GPS market', *Security Systems News*, vol.6, no.4, p.51.
- Gandy, O.H.J. 1993, *The Panoptic Sort: A political economy of personal information*, Westview Press, Boulder, Colorado.
- Garfinkel, S.L. 2000, *Database nation : the death of privacy in the 21st century*, O'Reilly, Beijing.
- Garfinkel, S.L., Juels, A. & Pappu, R. 2005, 'RFID privacy: an overview of problems and proposed solutions', *IEEE Security & Privacy Magazine*, vol.3, no.3, pp.34-43.

- Getting, I.A. 1993, 'Perspective/navigation-The Global Positioning System', *IEEE Spectrum*, vol.30, no.12, pp.36-38, 43-47.
- Goldstone, R. 2005, 'The tension between combating terrorism and protecting civil liberties', in R. Wilson (ed.), *Human Rights in the War on Terror*, Cambridge University Press, Cambridge, pp.157-168.
- Gottleib, C.C. & Borodin, A. 1973, *Social issues in computing*, Academic Press, New York.
- Gunther, O. & Spiekermann, S. 2005, 'RFID and the perception of control: the consumer's view', *Communications of the ACM*, vol.48, no.9, pp.73-76.
- Haneke, M. (2005). Cache.
- Harris, A.J. & Yen, D.C. 2002, 'Biometric authentication: assuring access to information', *Information Management & Computer Security*, vol.10, no.1, p.12.
- Hitchcock, A. (1954). Rear Window.
- Howitt, P. (2001). Antitrust.
- Hsi, S. & Fait, H. 2005, 'RFID enhances visitors' museum experience at the Exploratorium', *Communications of the ACM*, vol.48, no.9, pp.60-65.
- IIE Solutions 2002, 'Florida airport gets first RFID system', *IEE Solutions*, vol.34, no.7, p.14.
- Jain, A., Hong, L. & Pankanti, S. 2000, 'Biometric Identification', *Communications of the ACM*, vol.43, no.2, p.90.
- Jayakumar, S. & Senthilkumar, C. 2005, 'Biometric fingerprints based radio frequency identification', in P. Kantor, G. Muresan, F. Roberts, D. D. Zeng, Fei-Yue Wang, H. Chen and R. C. Merkle (eds), *Intelligence and Security Informatics*, Springer-Verlag Berlin Heidelberg, pp.666-668.
- Johnson, M.L. 2004, 'Biometrics and the Threat to Civil Liberties', *Computer*, vol.37, no.4, pp.90-92.
- Jones, P., Clarke-Hill, C., Hillier, D., Shears, P. & Comfort, D. 2004, 'Radio Frequency Identification in retailing and privacy and public policy issues', *Management Research News*, vol.27, no.8/9, p.46.
- Juels, A. 2006, 'RFID security and privacy: a research survey', *IEEE Journal on Selected Areas in Communications*, vol.24, no.2, pp.381-394.
- Kelly, E.P. & Erickson, G.S. 2005, 'RFID tags: commercial applications v. privacy rights', *Industrial Management + Data Systems*, vol.105, no.5/6, p.703.
- Kim, H.-J. 1995, 'Biometrics, is it a viable proposition for identity authentication and access control?' *Computers & Security*, vol.14, no.3, p.205.
- Kinsella, B. 2003, 'The Wal-Mart factor', *Industrial Engineer*, vol.35, no.11, p.32.
- Kun, L. 2004, 'Technology and policy review for homeland security', *IEEE Engineering in Medicine and Biology Magazine*, vol.23, no.1, pp.30-44.
- Langford, D. (ed.) 2000, *Internet ethics*, Macmillan, Basingstoke.
- Legner, C. & Thiesse, F. 2006, 'RFID-based maintenance at Frankfurt airport', *IEEE Pervasive Computing*, vol.5, no.1, pp.34-39.
- "liberty n." (2004). *The Australian Oxford Dictionary*. B. Moore. Oxford, Oxford

- University Press.
- “liberty” (1996). *The Oxford Dictionary of Philosophy*. S. Blackburn. Oxford, Oxford University Press.
- Louie, G. & von Eckhartsberg, G. 2006, ‘Security and liberty: how technology can bridge the divide’, in C. Northouse (ed.), *Protecting What Matters: technology, security, and liberty since September 11*, Brookings Institute Press, Washington D.C., pp.63-73.
- LSE (2005). The Identity Project: An assessment of the UK Identity Cards Bill & its Implications. London, London School of Economics and Political Science.
- Luban, D. 2005, ‘Eight fallacies about liberty and security’, in R. Wilson (ed.), *Human rights in the War on Terror*, Cambridge University Press, Cambridge, pp.242-257.
- Lynch, D. (1997). Lost Highway.
- Lyon, D. 2002, ‘Surveillance in cyberspace: the Internet, personal data, and social control’, *Queen’s Quarterly*, vol.109, no.3, pp.345-357.
- Mann, M. (2004). Collateral.
- McLean, D. 1995, *The Difficulty of Privacy as an Idea. Privacy and its Invasion*, Praeger Publishers, Westport.
- 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, K., McNamee, A., Michael, M.G. & Tootell, H. 2006a, ‘Location-Based Intelligence – Modeling Behavior in Humans using GPS’, in *Proceedings of the International Symposium on Technology and Society*, New York, IEEE Computer Society, 8-11 June 2006a
- Michael, K. & Michael, M.G. 2004. ‘The social, cultural, religious and ethical implications of automatic identification.’ *Proceedings of the Seventh International Conference in Electronic Commerce Research*, Dallas, Texas.
- Michael, K. & Michael, M.G. 2006a, ‘The proliferation of identification techniques for citizens throughout the ages’, in K. Michael and M. G. Michael (eds), *First Workshop on the Social Implications of National Security*, University of Wollongong, Wollongong, pp.7-26.
- Michael, K., Michael, M.G., Tootell, H. & Baker, V. 2006b, ‘The hybridization of automatic identification techniques in mass market applications: towards a model of coexistence’, in *Third International Conference on Management and Innovation*, Singapore, IEEE Computer Society, 21-23 June 2006b
- Michael, M.G. & Michael, K. 2006b, ‘National Security: The Social Implications of the Politics of Transparency’, *Prometheus*, vol.24, no.4, pp.359 - 363.
- Nath, B., Reynolds, F. & Want, R. 2006, ‘RFID Technology and Applications’, *IEEE Pervasive Computing*, vol.5, no.1, pp.22-24.
- Ng-Kruelle, G. & Swatman, P. 2002, ‘The price of convenience: privacy and

- mobile commerce', *Quarterly Journal of Electronic Commerce*, vol.3, no.3, pp.273-285.
- Niccol, A. 1997, 'Gattaca'.
- Northouse, C. (ed.) 2006, *Protecting What Matters: technology, security, and liberty since September 11*, Brookings Institute Press, Washington D.C.
- Oderwald, R.G. & Boucher, B.A. 1997, *Where in the World and What? An Introduction to Global Positioning Systems*, Kendall Hunt Publishing Company, Dubuque.
- OFPC (2006). Information Technology and Internet Issues. Office of the Federal Privacy Commissioner.
- Ohkubo, M., Suzuki, K. & Kinoshita, S. 2005, 'RFID privacy issues and technical challenges', *Communications of the ACM*, vol.48, no.9, pp.66-71.
- Orwell, G. 1949, *Nineteen eighty-four: a novel*, Secker and Warburg, London.
- Peckinpah, S. (1983). *The Osterman Weekend*.
- Perusco, L., Michael, K. & Michael, M.G. 2006, 'Location-based services and the privacy-security dichotomy', in *Third International Conference on Mobile Computing and Ubiquitous Networking*, London, 11-13 October 2006
- Petersen, J. 2001, *Understanding surveillance technologies: spy devices, their origins & applications*, CRC Press, New York.
- Poessl, S. 2006, *Indonesian Government unveils the World's most comprehensive, decentralized, biometric Passport Project, delivered by Digital Identification Solutions* accessed 4 August 2007, <http://www.findbiometrics.com/press-release/3440>
- Rankl, W. & Effing, W. 2000, *Smart Card Handbook*, John Wiley, Chichester, England.
- Relyea, H.C. 2002, 'Homeland security and information', *Government Information Quarterly*, vol.19, no.3, pp.213-223.
- Robinson, P.A. (1992). *Sneakers*.
- Rood, E.P. & Hornak, L.A. 2003, 'Are you who you say you are?' *The World & I*, vol.18, no.8, p.142.
- Rule, J., McAdan, D., Stearns, L. & Uglow, D. 1980, *The Politics of Privacy*, Elsevier Science Publishers, New York.
- Scheeres, J. 2005, 'When your mole betrays you', *Wired News*, no.19 September.
- Schoeman, C. 1992, *Privacy and Social Freedom*, Cambridge University Press, New York.
- Scorsese, M. (2006). *The Departed*.
- Scott, T. (1998). *Enemy of the State USA*.
- Smith, L. 2005, 'RFID Report', *The Humanist*, vol.65, no.3, p.37.
- Snow, D. 2004, *National Security for a New Era: Globalization and Geopolitics*, Pearson Education, Inc., New York.
- Spielberg, S. (2002). *Minority Report*.
- Srivastava, L. 2007, 'Radio frequency identification: ubiquity for humanity', *info*, vol.9, no.1, pp.4-14.

- Starner, T. 2001, 'The challenges of wearable computing: Part 2', *IEEE Micro*, vol.21, no.4, pp.54-67.
- Swartz, N. 2004, 'Tagging toothpaste and toddler', *Information Management Journal*, vol.38, no.5, p.22.
- The Royal Academy of Engineering (2004) "Response to the House of Commons Transport Select Committee: Inquire into Galileo." September 2004, accessed 4 August 2007, <http://www.raeng.co.uk/news/publications/list/responses/galileo.PDF>
- van der Ploeg, I. 1999, 'The illegal body: 'Eurodac' and the politics of biometric identification', *Ethics and Information Technology*, vol.1, no.4, pp.295-302.
- Want, R. 2004, 'Enabling ubiquitous sensing with RFID', *IEEE Computer*, vol.37, no.4, pp.84-86.
- Warren, S.D. & Brandeis, L.D. 1890, 'The right to privacy', *Harvard Law Review*, vol.4, no.5, p.193.
- Washington, D. (2006). *Deja Vu*.
- Weir, P. (1998). *The Truman Show*.
- Wenders, W. (1997). *The End of Violence*.
- Westin, A.F. 1967, *Privacy and Freedom*, Atheneum, New York.
- Westin, A.F. 2006, 'How the public sees the security-versus-liberty debate', in C. Northouse (ed.), *Protecting What Matters: Technology, Security, and Liberty since September 11*, Brookings Institute Press, Washington D.C., pp.19-38.
- Wigan, M. & Clarke, R. 2006, 'Social Impacts of Transport Surveillance', in K. Michael and M. G. Michael (eds), *First Workshop on the Social Implications of National Security*, University of Wollongong, Wollongong, pp.27-44.
- Winner, L. 1986, *The whale and the reactor: a search for limits in an age of high technology* University of Chicago Press, Chicago.
- Woodward Jr, J. 1997, 'Biometrics: privacy's foe or privacy's friend?' *Proceedings of the IEEE*, vol.85, no.9, pp.1480-1492.
- Woodward Jr, J. (2001) "Biometrics: facing up to terrorism." *RAND Issue Paper*, accessed 2 February 2006, http://www.rand.org/pubs/issue_papers/IP218/
- Wran, N. 2006, *Civil liberties: an endangered species*, accessed 1 March 2007, <http://lionelmurphy.anu.edu.au>
- Yeo, V. 2006, *S'pore unveils new biometric passport*, accessed 4 August 2007, <http://www.zdnetasia.com/news/security/0,39044215,39346963,00.htm>
- Zoreda, J.L. & Oton, J.M. 1994, *Smart cards*, Artech House, Inc., Massachusetts.

16

Privacy implications of automated GPS tracking and profiling

Muhammad Usman Iqbal¹ and Samsung Lim²

¹PhD Candidate, ²Senior Lecturer, School of Surveying and Spatial Information Systems, University of New South Wales

Abstract

Recent advancements in GPS technology have opened new avenues for its use in the automotive sector. While GPS is a self-positioning system and does not threaten 'locational privacy', its availability in telematics systems enables various privacy abuses both in real-time and retrospect. GPS devices are being used for surreptitious monitoring, for providing alibis and more recently, by the government to access telematics-generated GPS data for complementing their mass surveillance projects. While researchers have presented theoretical studies of privacy abuses and their countermeasures, limited research has been conducted to assess these threats in a real-life scenario involving data obtained from people. This paper aims to raise awareness about privacy issues created as a result of GPS-based surveillance by conducting an experiment involving collecting positional data from a number of volunteers. A software protocol is implemented which takes this GPS data as input and produces profiles of road behaviour, social activities and work activities of the volunteers. Interviews are conducted with the volunteers to assess the accuracy of this profiling. Results suggest that while these profiles can be highly predictive of personality traits, they may also be misleading due to technical limitations and inaccuracies. Positional data is highly detailed and it is important to negotiate the function, storage and use of such data so that future telematics systems do not impinge upon privacy rights of motorists.

Keywords: surveillance, location privacy, data-mining, threats, GPS, ethics, profiling, location tracking

1 Introduction

The automobile has gradually evolved from an analogue machine with mostly mechanical and hydraulic components to an electronic system with a growing number of computer-based systems. Within the realms of this 'smart car' revolution, GPS vehicle navigation has attracted significant attention from consumers. It is generally accepted that the automotive industry would be one of the largest consumers of GPS technology. There are efforts already underway to use this infrastructure for additional value added services, for instance, mobility-pricing of insurance (Tripsense 2007; Norwich Union 2007), infrastructure-less electronic toll collection and GPS-enabled parking fee collection (Grush 2005).

These applications would require disclosure of positional data by its users in real-time through a communications infrastructure. These systems would process the positional data to charge the motorist for the services rendered. A decrease in the cost of electronic storage means that this captured data intended for a specific purpose, originally transaction processing, may be retained indefinitely or at least for long periods of time. Since GPS data is information rich, the temptation to use it for secondary purposes may be too great to resist.

While theoretical research has aimed to raise awareness about these threats and proposed algorithms to protect the privacy of individuals in location contexts (Gruteser & Grunwald 2003; Duckham & Kulik 2005), limited research has been conducted to assess these threats in a real-life scenario involving data obtained from people. This paper aims to raise awareness about privacy issues created as a result of GPS-based surveillance by conducting an experiment involving collecting positional data from a number of volunteers. A software protocol is implemented which takes this GPS data as input and generates a range of personal information about the individual including their home addresses, social and work activities. The next section explores pertinent issues in the ethics of GPS and society, followed by a detailed explanation of the research study.

2 Background

2.1 GPS alibi and GPS-enabled surveillance

There have been instances where motorists have successfully challenged issuance of speed tickets against them by providing their GPS data as evidence. These cases have set a legal precedent to question the accuracy of hand-held radar guns (Wainright 2007). Even navigation equipment manufacturers are taking this opportunity to market their products as potential 'alibis'.

In other instances, legal precedents have also been set where the surreptitious installation and monitoring of GPS tracking devices does not require court orders (McCullagh 2005). The court ruled that the motorist has no expectation of privacy on a public roadway and it was legitimate for the police to perform surveillance of the vehicle without requiring a warrant. While warrants are not hard to acquire, they

offer some judicial oversight where law enforcement personnel have to contact a neutral magistrate or judge and justify their suspicions when engaging in the tactic of surveillance, preventing abuse of the system.

Yet again, manufacturers are cashing in on the opportunity by advertising their tracking devices for covert surveillance operations, e.g. for curious spouses and employers. As shown in figure 1, some manufacturers even explain graphically how to covertly install these devices (TrackStick Pro 2007). These ethical issues require the attention of researchers and policy-makers to provide rigorous ethical safeguards on GPS tracking procedures.

Additionally, whether used as an alibi, or to convict somebody of a crime, GPS data is not suitable in its current form as evidence (Michael, McNamee & Michael 2006). The reason is that GPS devices lack any cryptographic protection for the tracks, routes and waypoints stored on its memory, and a compatible software tool can be easily used to edit the positional data. Unless there are cryptographic techniques present to digitally sign the contents for non-repudiation, innocent people can be framed and convicted, and traffic offenders would escape paying for fines.



Figure 1: Covert installation of GPS tracking device

2.2 Mobility-pricing and überveillance

Mobility-pricing of insurance is a new approach that employs location technology allowing for the customisation of insurance premiums to more accurately reflect the risks based on actual vehicle usage. This would reduce the cross-financing of high risk drivers by low risk ones and increase fairness of insurance systems. There have been successful pilot studies conducted throughout the world that use GPS and telematics technology to offer actuarially accurate insurance products (Tripsense 2007; Norwich Union 2007). In the Australian context, a recent statement by an NRMA (National Roads and Motorists' Association) Insurance official lauded the benefits that GPS-based insurance would offer to motorists but also acknowledged the inherent "Big-Brother-ish" qualities that such a product would bring about

(NRMA 2007).

GPS logs are a form of data, and its monitoring would fall within the realms of informational surveillance. “Dataveillance”, a term coined by Clarke (1988) refers to the use of personal data in monitoring actions of communications of individuals. M.G. Michael’s work gives rise to the emerging notion of “überveillance”, an above and beyond almost omnipresent surveillance system (Michael et al. 2006). It is possible that mobility-based insurance would conveniently enable this pervasive surveillance and potentially have a chilling effect to the privacy rights of motorists. These issues would be further aggravated by the government’s interest in acquiring this data from insurance providers by offering them incentives. There is already speculation about this practice in the UK where an insurance company that offers mobility-pricing has been contacted by the government for data access for its own congestion charging scheme (Hytech 2007) in exchange for certain benefits. These developments, however, have not gone unnoticed by privacy researchers. Coroama and Langheinrich (2006) implemented a GPS based insurance system which calculates premiums on-board the vehicle guaranteeing privacy of owners. In this system, there is periodic transmission of aggregated information to the insurance provider for bill generation. Iqbal and Lim (2006) extended this idea further and proposed a GPS-based insurance product that preserves location privacy by computing distances travelled on the on-board unit and additionally safeguarded “spend privacy” by proposing smart card based anonymous payment systems.

2.3 Privacy in public

As mentioned in section 2.1, public surveillance has become a part of a modern citizen’s life. The ubiquitous presence of surveillance cameras, speed cameras and electronic toll collection booths digitises and stores the movement of motorists on various databases. Motorists relinquish the right to privacy to obtain the privilege of using the road networks. That is why ‘Privacy in public’ is a difficult concept to grasp. Past research and legislation has focused on the old adage, ‘A man’s home is his castle’, and has aimed to characterise privacy as a notion to protect an individual’s right in their homes against unreasonable searches and seizures (Krull, 1999). Not much attention has been given to the notion of ‘location privacy’. However, with emerging technologies that depend on GPS for their data processing, it is vital that adequate attention is paid to building a theory of privacy in public by drawing from existing legal frameworks and philosophical contexts.

Nissenbaum (2004) proposes the theory of ‘contextual integrity’ to tackle the complex issue of privacy in public. This theory is built around the notion that all realms of life are governed by norms of appropriateness and norms of distribution. Norms of appropriateness distinguish between intimate information that is appropriate to disclose and information that is inappropriate. Likewise, norms of distribution govern how personal information about somebody is shared with others. While norms of appropriateness would allow one to discuss relationship problems

with a close friend, the close friend would be violating the norms of distribution if s/he discloses this information to a third party. Contextual integrity is maintained when both the norms of appropriateness and norms of distribution are respected.

3 Research Motivation

3.1 Related Work

Location is an important aspect of context in pervasive computing, and has attracted considerable attention from researchers to extract “significant locations” from positional data. Significant locations may be the residential address, places of interest for an individual including preferred shopping centres or restaurants. Ashbrook and Starner (2003) used GPS data from a single volunteer collected over a four month period and used it to derive the locational context of a user. They developed an algorithm which extracted significant locations from the GPS data and used it to design an intelligent predictive model of the user’s future movements.

Krumm developed a similar protocol and tested it to identify the home location and infer identities of the volunteers. He collected the data from 172 individuals and used a reverse geo-coder to infer home locations of roughly 5% of the participants correctly. He then applied the theoretical countermeasures already present in location privacy research, such as spatial cloaking (Gruteser & Grunwald 2003), noise and rounding (Agrawal & SriKant 2000) on the GPS data and tested their effectiveness by quantifying how well these algorithms prevented the inference algorithms from finding the subjects’ home addresses.

Michael et al. (2006) used a combination of GPS receiver data and diary logs of a volunteer over a period of two weeks to seek an understanding of the social implications of tracking and monitoring subjects. Their research identifies the ethical dilemmas associated with use of GPS on civilians and points out that adequate safeguards need to be placed to avoid abuse of information gathered through GPS technology.

In terms of driving behaviour, Greaves and De Gruyter (2002) discuss how a driving profile of a person can be derived from GPS track data. They sought an understanding of driving behaviours in real world scenarios by fitting low-cost GPS receivers to vehicles, and logging the vehicle movements. Consequently they were able to identify driving styles from this data.

3.2 Motivation

Previous sections have set the theoretical stage for conducting a privacy assessment of GPS tracking. This paper is one of the first efforts to collect and analyse location data from multiple volunteers and generate automated profiles without human intervention. This motivation comes from the fact that it would be cumbersome to analyse GPS data of a large number of individuals on a manual basis.

The attack model simulates a typical adversary’s three main moves. The first

step is information collection using passive surveillance. This step is followed by information processing by using data-mining, pattern recognition, and reverse geo-coding of significant locations. Finally in the third step, the adversary performs information dissemination by creating summary profiles.

4 Research study

4.1 Surveillance

In order to mimic truly surreptitious surveillance, a GPS tracking device was required that worked without any input and intervention from the users. The selection process led to choosing a passive GPS device known as the Trackstick Pro as shown in figure 2. This GPS stick uses power from the cigarette lighter in the car and has a memory of 4 megabytes, which is suitable for storing the track data for up to a period of one month.



Figure 2:
The GPS device used



Figure 3:
Installed and operational

A total of five volunteers were selected for this study. The sample consisted of an undergraduate student, a research student, an academic staff member, and two support staff from the school. Before the study began it was hypothesized that different types of people would have different patterns, so a sample space was drawn that represented the different communities at the university. As shown in figure 3, volunteers were shown how to attach the GPS stick to their vehicle's dashboard using double sided tape and the cigarette lighter plug in the cigarette lighter jack. The GPS device had to be placed such that the globe would face up, as shown in figures 2, and 3. The volunteers were advised not to remove the stick or the power source for the period of study. At least one week's worth of data was collected from all the volunteers. The sticks were circulated and collected on Wednesdays to include both weekend and weekday driving. It was expected that the passive nature of the device would yield data closest to the actual driving attitude of the volunteers and would not result in behaviour modification on their part.

The GPS device was configured to be used in a vehicle through the software drivers present on the PC (Personal Computer). On the average it logged location,

time, date, speed, elevation and temperature data at a rate of 6 times per minute. Although the desired logging rate would have been on a per second basis, the TrackStick is not capable of logging at such a high rate. Ultimately, this option was chosen as a trade-off between granularity and convenience for the volunteers. On completion of the specified period, the GPS data was downloaded to the PC and stored anonymously without identifying the volunteer in any way.

4.2 Information Processing and dissemination

4.2.1 Home and work location identification

The first step in the analysis is to identify significant locations from the data. As shown in figure 4, the GPS device logs the status as “Power Off” when the ignition of the vehicle is switched off. The data row prior to this event (marked with a red circle) has a significant location since this is the last known position before the vehicle stopped. Note that the speed for the record is not zero as the tracking device roughly logs around 6 times per minute. This means that the actual parking position can be metres away. This inaccuracy requires softening the location identification algorithm and including a buffer of 4 properties around the one that the solution finds to be the valid address of the volunteer.

Rec #	Date	Time	Latitude	Longitude	Altitude	Status	Course	GPS Fix
134	03/17/2007	11:15	-33.9120°	151.1194°	24.7 m	31 kph	NE	Y
135	03/17/2007	11:15	-33.9116°	151.1199°	25.4 m	31 kph	NE	Y
135	03/17/2007	11:15	----	----	----	Power Off	----	----
140	03/17/2007	11:22	----	----	----	Power On	----	----
141	03/17/2007	11:22	-33.9054°	151.1275°	0.0 m	0 kph	N	Y

Figure 4: GPS track data downloaded onto PC from GPS device

The algorithm is implemented in Visual Basic.net. The purpose of choosing this programming language is that there are APIs (Application Programming Interfaces) available in this language that would programmatically allow connecting to the GIS (Geographical Information System) software for further analysis and profiling. The algorithm selects all the locations prior to the “Power Off” signal in an effort to identify the home locations. Since all the volunteers are associated with the university, the algorithm does not compute the work locations and concentrates in identifying home locations only. The algorithm uses certain heuristics so that on weekdays, it is weighted to give higher importance to significant locations during the period between 3 PM – 10 PM. This rule is based on the fact that most people’s trips would end at their home locations during this time period.

To find the nearest street address to the significant locations, PSMA (Public Sector Mapping Agencies) Australia’s GNAF (Geo-coded National Address File) index is used. This address file contains the geocode (specific latitude and longitude) of all physical addresses in Australia. This data is stored in a spatial database capable of

performing spatial queries. PostGIS which spatially enables the PostgreSQL database server is used to store the GNAF data, since it is open-source and reliable to use. Due to the magnanimity of storage requirements, GNAF data for only New South Wales is loaded into the database which requires 5 gigabyte of storage space alone.

Table 1: Protocol output of inferred home locations with actual addresses obtained from interviewing volunteers.

Home location	Volunteer C	Volunteer B	Volunteer Y	Volunteer J	Volunteer U
Street number(s) inferred	7	39	24, 25	44	53
Actual street number	11	39	22	Different street	51

Using Spatial SQL (Structured Query Language) the filtered significant positions (through time heuristics) are queried from the database. The output is a set of physical addresses. The statistical mode is used to short-list the physical address of the volunteers. Since the mode is not necessarily unique, the physical address computed by the protocol may be more than one. Table 1 summarises the protocol output at this stage. Only initials of the volunteers are used to keep their details anonymous. For Volunteer B, the inferred address was the actual street address. For three out of the remaining four volunteers (C, Y, U), the physical address computed was the next door address where they actually lived, which according to the assumption falls within the 4 address buffer range. For Volunteer J, the physical address computed was on a parallel street. The logical explanation for this is that the volunteer parked his car in an underground car park and entered the street through a parallel street so the last significant position is recorded on the road closest to the proposed street address as shown in figure 5. The volunteers were shown a list of all the computed addresses and asked to find out the closest one to their address.

4.2.2 Profile generation

After inferring the street address of the drivers, the next stage is to use the same data and make inferences about their social and work related activities. The whole GPS track data is sifted and aggregated, and the output of this step is summarized in table 2. While this list is not exhaustive, it is evident that a lot of calculated guesses can be made about individuals based on this data. Inferences can be drawn about how long a person spends time at work, and what times the person is not at their home. This information can be used by adversaries with malicious intent. Krumm (2007) has furthered this idea and computed relative probabilities of the times when a subject may be home. Additionally the speed and travelled distance details indicate how long a person stays on the road and the average distance travelled each day.

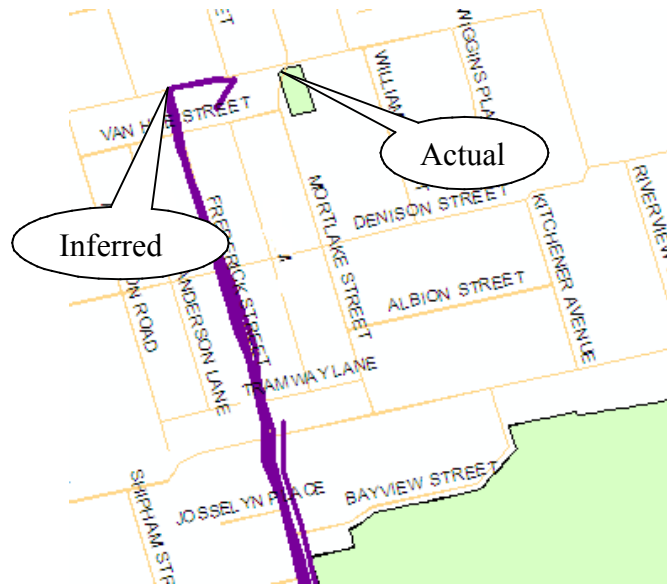


Figure 5: Street address for volunteer incorrectly guessed by the home determination algorithm

Volunteer Y seems to spend the longest time at the university, and lives the farthest distance. On average he/she has to travel approximately 40 kms to commute to work and back home each day. The algorithm is also designed to guess the profile type of the individual with the GPS. For example, a rule that is incorporated in the protocol is that a person spending a great amount of time at university is most likely a research student. Likewise, a person who has a vehicle and does not park at the university parking lot is not privileged with a parking permit. Another heuristic used is that if a person parks within 1 km buffer around the university, then he/she does not have a parking permit and is most likely an undergraduate student. While these heuristics have proven to be true in this particular case, they may not necessarily always be valid. For instance, there might even be an academic staff member who is putting in extra hours to prepare lecture material for the forthcoming semester. Under the present algorithm, he/she would be identified as a research student.

Further inferences can also be drawn using this data to determine social networks, for instance Wigan and Clarke (2006) have highlighted issues related to location tracking and social networks. They argued that continuous tracking of vehicles can produce trails which can tell where a person currently is. This information can be correlated to another person's location at the same time to probabilistically infer social networks. Additionally, the routes that a person takes to reach different destinations can also provide crucial information to their individual pattern.

**Table 2: Profile summary of volunteers
generated by the software protocol**

Work and commute profile	Volunteer C	Volunteer B	Volunteer Y	Volunteer J	Volunteer U
Total GPS records	5240	1997	2330	4812	2147
Total Distance	301 km	174.59 km	172 km	284.9 km	149.72
Average distance	27.38 km	34.59 km	31.2 km	40.7 km	37.43 km
Total travel time	12 hr 45 m	4 hr 25m	5 hr 1 m	11 hr 44 m	4 hr 51 m
Average travel time	1hr 10 m	52 m	54 m	1 hr 40 m	1 hr 12 m
Max Speed	101 kph	83 kph	86 kph	98 kph	91 kph
Average Speed	32 kph	45 kph	39 kph	33 kph	39 kph
Average time leaves home	7:33 am	8:21 am	9: 10 am	07:46 am	9:54 am
Average time leaves work	3:30 pm	5:09 pm	4:54 pm	08:58 pm	5:07 pm
Average time arrives at work	8:03 am	8:55 am	9:32 am	08:40 am	10:15 am
Average time at work	7 hr 58 min	8 hr 10 min	7 hr 25 min	12 hr 18 m	6 hr
Parks car in	University parking lot	University parking lot	University parking lot	University parking lot	Around university
Type of person	Academic Or Support	Academic Or Support	Academic Or Support	Research Student	Undergrad Student

4.2.3 Driver behaviour analysis

In this section speed and acceleration analysis is carried out. While the algorithm produced speed and acceleration graphs, as well as speed maps for all the volunteers, for the sake of clarity and brevity, only one volunteer's data is discussed.

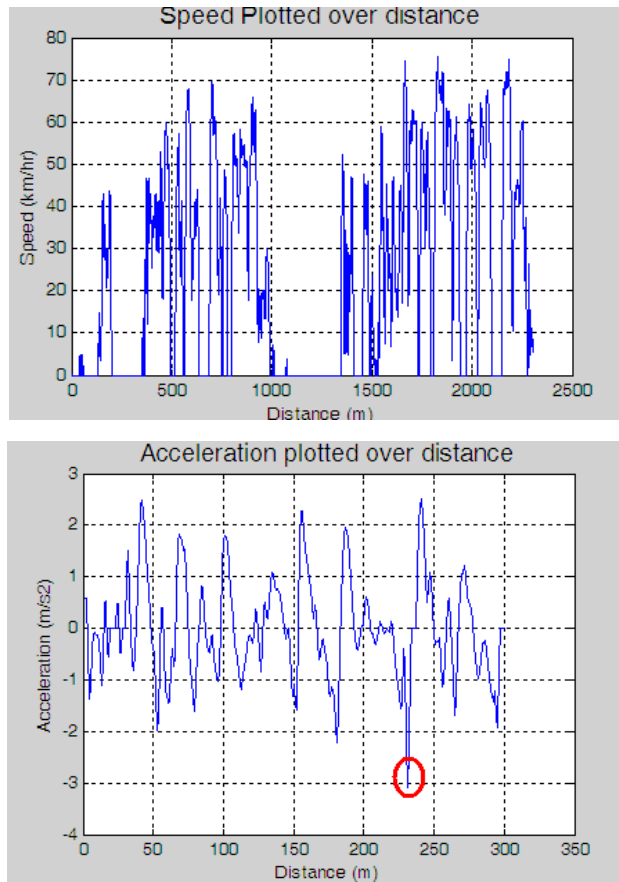


Figure 6: Speed and acceleration graphs for volunteer

Intuition suggests that individual driving behaviour is a function of many factors such as characteristics of that individual, for instance, the driver's age, gender, purpose of trip, the type of vehicle and reported traffic conditions. It is also widely acknowledged that higher speeds increase the likelihood and severity of collisions (Kloeden et al. 1997). The purpose of this section is to demonstrate that GPS data can be used to make inferences about an individual's driving behaviour. This road activity analysis was carried out by generating speed and instantaneous acceleration graphs as well as detailed speed maps of trip data where speed variability is represented using different colours on GIS maps. As mentioned earlier, VB.net was used to programmatically access the GIS APIs for dynamically constructing the required maps of speed data. The road network data was obtained from PSMA's "Transport and Topography" dataset. This dataset was in MapInfo format, and had to be converted to ESRI compliant format using a freely available conversion tool.



Figure 7: Speed profile of volunteer using waypoint data

In this stage, the GPS data was programmatically converted to ESRI Shapefile format, which is the preferred file format for ArcGIS. Version 9.2 of ArcGIS was used. All the records from the GPS data that had a status of “Power On” were removed as they had no positional information and could not be used on the map. The points with the “Power Off” status were edited in this process to have positional information of its preceding GPS record. These would prove useful in demonstrating the idea of significant locations mentioned in the location identification section. The resultant output was two sets of Shapefiles, one for the GPS track and the other for GPS waypoints respectively.

Figure 6 shows the speed and acceleration graphs plotted for a particular volunteer. It can be observed in the acceleration sub-graph that the individual had to decelerate the vehicle at -3 m/s^2 at a certain stage, which is considered risky according to prior research (Watson 1995; Greaves & De Gruyter 2002). In terms of environmental impacts, even though the impact of overall driving styles may be less obvious, high speeds (80 kph and above), rapid accelerations and decelerations of more than $\pm 3 \text{ m/s}^2$ are considered to be a source of increased fuel consumption and emissions and may indicate the driving behaviour of individuals.

Figure 7 represents the routes the individual took from the home location to the university. The black dots on the map indicate significant locations that were used to infer home locations. Note the black dots around the university vicinity, where the volunteer had parked the car frequently and were used to predict if the volunteer was an undergraduate student. The red dots indicate that the speed with

which the car was being driven was greater than 80 kph. With access to speed data of all the roads, it can be easily correlated to find if an individual was over the speed limit. It is also not hard to imagine that if insurance companies get access to this data, they would use this information, in order to identify an individual with an 'aggressive' driving style. The insurance provider can then assign the individual a higher risk, leading to a higher premium or denied motor insurance altogether (Iqbal & Lim 2006).

5 Discussion

Using an adversarial attack paradigm, the protocol involved information collection using surveillance, information processing using data-mining and information dissemination using spatial maps and tabular reports. The profiling exercise looked at various aspects of the volunteers' lives and predicted what class of personnel they belong to (academic staff, support staff, graduate student or undergraduate student). The protocol also identified the residential address of 4 out of 5 volunteers within the specified spatial granularity. The protocol further characterised the road behaviour of volunteers by looking at speeds and accelerations.

While results suggest that these profiles can be highly predictive of personality traits, they may also be misleading due to various reasons. For instance, one of the heuristics used was that the person spending the most time at university is most likely a graduate student. Spending more time at the campus doesn't necessarily mean that one is at work. A student may be involved in extra-curricular activities or work on campus cafes and bookshops. Similarly, an academic may be on campus for extended periods of time preparing lectures for the forthcoming semester or applying for a research grant.

Future telematics applications would work on location data in order to provide services. For instance mobility pricing of insurance (Norwich Union 2007), which brings the concept of "fairness" to insurance premiums would require disclosure of positional to generate per-mile premiums. However, there would also be unintentional transmission of data that may be used against the motorist, for instance how hard one brakes/accelerates or how often one goes above the speed limit. One solution to avoid these abuses is to aggregate the GPS data and send only the information necessary for premium calculations. A similar privacy-aware system recently identified is the GM FleetView (2007), which is primarily for fleet management, but has built-in privacy features. Employees may find such systems quite useful to track work-related travel for tax purposes; however, these individuals operating such vehicles have a reasonable expectation of privacy when using the vehicles after-hours. This system has a toggle switch in the vehicle which an employee can select to identify a business or personal trip. Location of the vehicle would not be transmitted when driving in personal mode. To conclude, it is imperative that future telematics systems respect the privacy of motorist and provide configurable features for motorists to opt-out or opt-in on a more granular scale.

6 Conclusion

The purpose of this experiment is to demonstrate that GPS data can be used to draw numerous inferences about individual personality traits by a simple click of a button. These inferences can be used to harm an individual and may prove embarrassing to him/her when revealed publicly. Future invasions of privacy in location contexts would employ technologies presented in this paper. With the recent trend of installing GPS chips in mobile phones in order to accessorize them with navigation features (Roche 2007), one should ask what safeguards have been provided that mobile phones cannot be remotely hacked to gain access to this data? With accounts of law enforcement officials remotely activating mobile phones of suspects for audio surveillance (McCullagh & Broache 2006), it is not hard to imagine that the GPS data could also remotely and surreptitiously be read providing a ubiquitous surveillance device. The combination of motorists and mobile phone users form a huge majority of the urban population and citizens should not be victims of mass surveillance or privacy abuses based on location data. Rigorous ethical and legislative safeguards need to be implemented to protect future abuses of individuals' privacy in this context. Location technologies are still in their nascent stages, therefore, from a technology point of view, it is important to dispel these privacy concerns right from the beginning, and focus on "building in" privacy protection within such systems so that as new applications become available, appropriate privacy measures are integral to them.

Acknowledgements

The author wishes to acknowledge the financial assistance provided by the 'Metadata Scholarship' from OMNILINK Pty. Ltd. for this research.

References

- Agrawal, R & Srikant, R 2000, 'Privacy-Preserving Data Mining', in ACM SIGMOD Conference on Management of Data. Dallas, TX, USA: ACM Press.
- Ashbrook, D & Starner, T 2003, 'Using GPS to Learn Significant Locations and Predict Movement across Multiple Users', *Personal and Ubiquitous Computing*, 2003. 7(5): pp. 275-286.
- Clarke, RA 1988, 'Information Technology and Dataveillance', *Communications of the ACM*, 31(5), 1988, pp. 498-512.
- Coroama, V & Langheinrich, M 2006, 'Personalized Vehicle Insurance Rates – A Case for Client-Side Personalization in Ubiquitous Computing', Paper presented at the *Workshop on Privacy-Enhanced Personalization* at CHI 2006, Montréal, Canada, 22 April, 2006.
- Duckham, M & Kulik, L 2005, 'A Formal Model of Obfuscation and Negotiation for Location Privacy'. *Lecture Notes in Computer Science*, 3468, pp. 152-170.

- GM Fleetview 2007 GM FleetView Presentation Video, viewed 18th March 2007, <http://video.vividas.com/media/4630_GMFleet/web>
- Greaves, SP & De Gruyter, C 2002, 'Profiling driving behaviour using passive Global Positioning System (GPS) technology' presented at *Institute of Transportation Engineers International Conference*, Melbourne, Australia.
- Grush B 2005, 'Optimizing GNSS-Based Mobility Pricing for Road-Use, Parking, and PAYD Insurance', *4th European Traffic Congress*. Salzburg, Austria
- Gruteser, M & Grunwald, D 2003, 'Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking', Paper presented at the *First International Conference on Mobile Systems, Applications, and Services*, San Francisco, USA.
- Hytech D 2007, 'Service vendors target traffic-management deals', *Computer Business Review Online*, viewed 25 July 2007, <http://www.computerbusinessreview.com/article_news.asp?guid=E01E9184-2F51-4B85-9577-D0A6C72AF895>
- Iqbal, MU & Lim, S 2006, 'A privacy preserving GPS-based Pay-as-You-Drive insurance scheme', *Symposium on GPS/GNSS (IGNSS2006)*. Surfers Paradise, Australia, 17-21 July, CD-ROM proceedings.
- Kloeden, CN, McLean, AJ, Moore, VM and Ponte, G 1997, 'Travelling speed and the risk of crash involvement', *Report CR 172*. Federal Office of Road Safety, Canberra.
- Krull, K 1999, *A Kid's Guide to America's Bill of Rights*, pp. 224, New York, Avon Books.
- Krumm, J 2007, 'Inference Attacks on Location Tracks', *Fifth International Conference on Pervasive Computing (Pervasive 2007)*, May 13-16, 2007, Toronto, Ontario, Canada.
- McCullagh, D 2005, 'Snooping by satellite', *CNET News*, viewed 29 July 2007, <http://news.com.com/Snooping+by+satellite/2100-1028_3-5533560.html>
- McCullagh, D & Broache, A 2006, 'FBI taps cell phone mic as eavesdropping tool', *CNET News*, viewed 10 April 2007, <http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029_3-6140191.html>
- Michael, K, McNamee, A & Michael, MG 2006, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring', in *Proceedings of the International Conference on Mobile Business*, Copenhagen, Denmark, 25-27 July 2006. IEEE Computer Society.
- Michael, K, McNamee, A, Michael, MG & Tootell, H 2006, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS', in *Proceedings of the International Symposium on Technology and Society*, New York, 8-11 June 2006. Copyright IEEE Computer Society.
- Nissenbaum, H 2004, 'Privacy as contextual integrity', *Washington Law Review*, 79 (1), 119-157.

- NRMA 2007, 'NRMA calls for car surveillance via GPS', *Ninemsn Science and technology news*, viewed 10 July 2007, <<http://news.ninemsn.com.au/article.aspx?id=59964>>
- Norwich Union Pay As You Drive Car Insurance, viewed 5 June 2007, <<http://www.norwichunion.com/pay-as-you-drive/index.htm>>
- Roche, J 2007, 'Nokia N 95', *CNET News*, viewed 28 July 2007, <<http://www.cnet.com.au/pdas/gps/0,239035573,339271384,00.htm>>
- TrackStick Pro, TrackStick Pro userguide, pp 30, viewed 12 April 2007, <http://www.trackstick.es/files/STS_user_guide.pdf>
- Tripsense, How TripSensor Works, viewed 11 January 2007, <<https://tripsense.progressive.com/about.aspx?Page=HowDeviceWorks>>
- Wainright R 2007, 'Father and son stick to guns to prove radar wrong', *Sydney Morning Herald*, viewed 5 July 2007, <<http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html>>
- Watson, HC 1995, 'Effects of a Wide Range of Drive Cycles on the Emissions from Vehicles of Three Levels of Technology', *Global Emissions Experiences*, SAE, Warrendale, Pa., USA. SP-1094, p. 119-132.
- Wigan, M & Clarke, R 2006, 'Social Impacts of Transport Surveillance', *Prometheus*, 24, pp. 389-403.

17

Human tracking technology in mutual legal assistance and police inter-state cooperation in international crimes

Katina Michael

Senior Lecturer, School of Information Systems and Technology, University of Wollongong

Gregory Rose

Associate Professor, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

The objective of this paper is to explore the role of human tracking technology, primarily the use of global positioning systems (GPS) in locating individuals for the purposes of mutual legal assistance (MLA), and providing location intelligence for use in inter-state police cooperation within the context of transnational crime. GPS allows for the 24/7 continuous real-time tracking of an individual, and is considered manifold more powerful than the traditional visual surveillance often exercised by the police. As the use of GPS for human tracking grows in the law enforcement sector, federal and state laws in many countries are to a great extent undefined or even contradictory, especially regarding the need to obtain warrants before the deployment of location surveillance equipment. This leaves courts ruling on transnational crimes in the precarious position of having to rely on age-old precedents which are completely void to the new capabilities of today's tracking technologies. On one side of the debate are civil libertarians who believe the individual's right to be let alone is being eroded to the compromise of human rights, and on the other side are law enforcement agencies who wish to provide more precise evidence to judges and juries during hearings against suspects (particularly in issues pertaining to national security). This paper argues that there is a radical middle position, the *via media*: that a warrant process is legislatively defined and not only for MLAs but also to formalise existing informal inter-state police cooperation. Safeguards are required to overcome the potential misuse of human tracking technologies by police officials and others in positions of power. And this particularly in light of the emerging implantable high-tech identification and tracking devices now commercially available.

Keywords: inter-state police cooperation, law enforcement, intelligence, global positioning systems (GPS), human tracking, covert surveillance, privacy, human rights

1 Mutual legal assistance in locating the accused

Mutual Legal Assistance (MLA)¹ can be defined as a mechanism by which lawyers and the courts of one jurisdiction can request assistance from another. MLAs ensure that individuals cannot evade prosecution simply because the evidence to prosecute them is located in another country. The MLA document states the required assistance sought in the provision of evidence for criminal proceedings or proceedings about to commence.² Depending on the domestic law and that law of the requested State, the most common types of assistance that is usually obtained includes: witness interviews and material held by third parties (such as telecommunication documents, phone records, e-mail, facsimile billing and subscriber information).³ This paper deals with the latter and specifically the use of covert location-based surveillance. MLAs should be used when evidence cannot be gathered using informal police-to-police cooperation.

In the treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, the scope of assistance ranges from ‘providing documents, records, and other articles of evidence; locating or identifying persons; and executing requests for searches and seizures and for restitution’.⁴ ‘These forms of legal assistance can be conducted by the judicial, prosecutorial or law enforcement personnel of the requested state.’⁵ Mutual Legal Assistance Treaties (MLATs) can be bilateral or multilateral.⁶ ‘As of the 1960s, the practice of many states (within Europe, Latin America, the United States, and Canada) shifted to bilateral MLATs... Still the number of bilateral MLATs is far less than bilateral extradition treaties, as is the number of states having national legislation

1 Mutual legal assistance was developed during the 1960s but its origins can be found in the century-old practice known as “Letters Rogatory.” Letters Rogatory is based on the principle of comity, when the ‘... courts of one state address a request to those of another state for judicial assistance in the form of taking the testimony of a witness or securing tangible evidence.’ See M. Cherif Bassiouni, *Introduction to International Criminal Law*, International and Comparative Criminal Law Series (2003) 352. See also Ilias Bantekas and Susan Nash, *International Criminal Law* (2003) 231. MLAs abide by the *locus regit actum* rule.

2 International Association of Prosecutors, *Basic Guide to Prosecutors in Obtaining Mutual Legal Assistance in Criminal Matters* (2004) 2.

3 Ibid. See also, the *Mutual Assistance in Criminal Matters Act 1987* (Cth). This Act should be read together with the following relevant Australian legislation: *Foreign Evidence Act 1994* (Cth), *Proceeds of Crime Act 2002* (Cth), *Telecommunications (Interception) Act 1979* (Cth), and the *Surveillance Devices Act 2004* (Cth). Only by studying the various Acts can one appreciate the complexity of MLATs and the various considerations that need to be grasped in making a request to a given state, or satisfying a request by another state.

4 Department of Foreign Affairs and Trade, *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, and Exchange of Notes* (2000).

5 Bassiouni, above 1, 354.

6 The 1959 Council of Europe Convention on MLA in Criminal Matters which was ratified in 1962 was one of the first multilateral treaties and is recognized as an important step in international judicial co-operation. See Bantekas, above 1, 234.

on the subject...⁷ States have become increasingly willing to negotiate MLATs,⁸ particularly since 11 September 2001 (9/11), as a means to increased access of evidence located abroad.⁹

What is unique about MLATs is that they are only really meant to benefit governments, and only governments can make exclusive use of evidence to satisfy a given request. However, governments are under no obligation to provide evidence and they can reject a request based on any number of grounds.¹⁰ MLATs in most instances contain provisions for human rights but through reservations and safeguards which are 'built-in' to protect the accused. It is important to note, that MLAs can only be executed by remaining in accordance with the law of the requested state, without violating third party rights. In the context of search for and seizure of evidence using location surveillance, this becomes very important.¹¹

2 Inter-state police cooperation for information gathering and sharing

Given the number of requests published in annual reports by government agencies, and the highly publicized media accounts of increasing transnational crime,¹² it is obvious that the collection and exchange of relevant information pertaining to a transnational criminal investigation happens through informal police cooperation at a federal level.¹³ One can conclude from this that mutual assistance and police-to-police assistance are complementary. However, while law enforcement and

7 Bassiouni, above 1, 353.

8 Bantekas, above 1, 231.

9 See, eg, Attorney-General's Department, *Annual Report 2004-2005* (2005) <[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(CFD7369FCAE9B8F32F341DBE097801FF\)~80Recent+Statistics.pdf/\\$file/80Recent+Statistics.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~80Recent+Statistics.pdf/$file/80Recent+Statistics.pdf)> at 1 June 2007. The number of requests made by Australia carried forward from 2003-04 were 170, new requests made in 2004-05 were 151, requests finalized were 126, and requests continuing were 195. The majority of requests came from the United Kingdom, Netherlands, and the United States of America, and the majority type of assistance granted was for telecommunications and email records etc, and bank and business records. A similar number of requests were made to Australia, indicating that MLATs are highly reciprocal in nature.

10 Bassiouni, above 1, 354.

11 Bantekas, above 1, 233-234. See also, *Model Treaty on Mutual Assistance in Criminal Matters*, adopted by General Assembly resolution 45/117, subsequently amended by General Assembly resolution 53/112 (entered into force 14 December 1990). In the context of human rights, see, Ian Brownlie and Guy S. Goodwin-Gill (es), *Basic Documents on Human Rights* (2002).

12 See, United Nations Office on Drugs and Crime, *The Seventh United Nations Survey on Crime Trends and the Operations of Criminal Justice Systems (1998 - 2000)*, (2006) <http://www.unodc.org/unodc/crime_cicp_survey_seventh.html> at 4 June 2007. Compare with data found in Attorney-General's Department, above 9. The statistics for MLAs and national/international crime trends indicates that a great number of investigations do not go through the MLA process but via the more informal police-to-police cooperation route.

13 Bantekas, above 1, 236, 261. 'Despite the increased willingness of States to engage in formal methods of mutual legal assistance, there are many other less formal methods of evidence gathering, which permit law enforcement agencies to exchange information and material relevant to transnational investigations.'

intelligence cooperation is increasing, it is not regarded in the same way from a legal perspective. For instance, there are no treaties applicable to law enforcement or police cooperation as there are for mutual assistance, nor are there codes of conduct for how information should be gathered and shared between government agencies.¹⁴ When one considers the need for location surveillance¹⁵ and other forms of covert surveillance, particularly in the gathering of evidence, '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.'¹⁶ In fact, regulation is the major problem here. How are potential abuses combated¹⁷ and how is effectiveness maintained? How can the accuracy of information be guaranteed? And what of privacy when international practices vary greatly? These are the challenges that new technologies and emerging law enforcement workflows pose on the due process of law.

As any other organization in a given jurisdiction, law enforcement agencies are bound by national criminal law at the domestic level. Yet, many have questioned whether this is enough given that intelligence and law enforcement agencies have been quite secretive about their practices. For the greater part the way that these particular organizations have shared intelligence has been outside legal or judicial supervision.¹⁸ Thus, the problem is two-fold: (i) a legal framework in most jurisdictions does not exist to aid in regulation, and (ii) there is a reluctance of members of the intelligence sector to provide transparency in their activities within a judicial system.¹⁹ This issue has been exacerbated since 9/11 when the United States demanded that states share more information with them, and that their intelligence

14 Bassiouni, above 1, 368. Bassiouni is strong in his stance commenting: '[r]egrettably, this important form of international cooperation [ie police cooperation in transnational crime] has not yet been included in mutual legal assistance treaties.'

15 Katina Michael et al, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS' (2006) *International Symposium on Technology and Society (ISTAS '06)* 1.

16 Bassiouni, above 1, 369. See also, Commission New South Wales. Law Reform, *Surveillance: An Interim Report* (2001).

17 John S. Ganz, 'Comment: It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices' (2005) 95 *Journal of Criminal Law & Criminology* 1360. 'Finally, again from a policy perspective, some might argue that the failure to require warrants could lead to arbitrary and capricious use of GPS by police. As dissenting Nevada Supreme Court Justice Robert Rose noted in Osburn, "The automobile's use is a necessity in most parts of Nevada, and place a monitor on an individual's vehicle effectively tracks that person's every movement just as if the person had it on his or her person... I fear that in some instances, the monitor will be used to continually monitor individuals only because law enforcement considers them "dirty." In the future, innocent citizens, and perhaps elected officials or even a police officer's girlfriend or boyfriend, will have their whereabouts continually monitored simply because someone in law enforcement decided to take such action. This gives too much authority to law enforcement and permits the police to use the vehicle monitor without any showing necessity and without a limit on the duration of the personal intrusion.'"

18 Bassiouni, above 1, 369.

19 Ibid.

personnel gather more data so as to curb such terrorist²⁰ acts in the future.²¹ Recent events have shown the power of data accessibility, with numerous terrorist plots foiled by intelligence organizations, preventing mass casualties.²² But at the same time the rights of individuals to know that data is being collected about them, to be able to rectify erroneous data, to protect privacy is also important.²³ The whole debate over weapons of mass destruction (WMD) allegedly located in Iraq, which was later proven to be unreliable, indicated the systemic flaws in American intelligence which were blamed primarily on management.²⁴ Interestingly, the result of this flaw, quite legitimately, was for American intelligence agencies to increase information sharing even more.²⁵ One can be lead to the hypothesis that greater intelligence effectiveness is proportional to the amount of information shared by states but this too has implications for privacy. Not only is the balance between personal privacy and national security almost impossible to achieve but intelligence born from “überveillance-type” regimes can introduce the potential for misinformation and misinterpretation. Going to one extreme or the other has negative implications- i.e. making all personal data public might increase transparency in the short-term but may have the equal effect of increasing identity fraud in the long-term, and not engaging in any information sharing practices would be detrimental to a nation’s security.

20 For comparative definitions of terrorism see, Claire De Than and Edwin Shorts, *International Criminal Law and Human Rights* (2003) 231-237.

21 Terrorism is considered to be just one reason why information gathering and sharing practices have increased, other notable transnational crimes include: drug and people trafficking, money laundering, and the smuggling of things. See eg, the role of intelligence in security informatics in Hsinchu Chen, *Intelligence and Security Informatics for International Security* (2006).

22 See, eg, Transportation Security Administration, *Information on Plot to Attack John F Kennedy Airport* (2007) <http://www.tsa.gov/press/happenings/jfk_terror_plot.shtm> at 2 June 2007.

23 Bassiouni, above 1, 370. There are however efforts between nations to broker agreements that do try to address data protection principles, at least in theory. See, eg, *Agreement Between the United States of America and the European Police Officer*, Europol file no. 3710-60r2 (Dec 6, 2001), *Supplement Agreement Between the United States of America and the European Police on the Exchange of Personal Data and Related Information*, Europol file no. 3710/60r3 (Dec. 20, 2002). “Europol is essentially a police coordination centre for collecting, analyzing and sharing information to help investigations being carried out in two or more EU countries”. European Commission, *Freedom, Security and Justice for All* (2004) 19. See also, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1981).

24 GlobalSecurity.org, *Intelligence: Additional Views of Senator Olympia Snowe* (2004) <http://www.globalsecurity.org/intell/library/congress/2004_rpt/iraq-wmd-intell_olympia-snowe.htm> at 3 June 2007.

25 Ibid. ‘Surprisingly, the Committee’s review reveals that even after the lack of information sharing was found to have played a key role in the intelligence failures of September 11, 2001, intelligence agencies still fail to share information within and among its own cadre. ... For example, the CIA failed to share information on the reliability of two biological weapons sources with all Iraq biological weapons analysts. Information about the credibility of these sources, upon which many assumptions regarding Iraq’s biological weapons program were made, could have significantly altered analysts’ judgments. In addition, the CIA failed to share some intelligence reporting with other agency [unmanned aerial vehicle] UAV analysts on critical issues surrounding Iraq’s UAVs. ... The Committee’s review shows that the CIA continues to overly compartment sensitive HUMINT reporting and that this lack of information sharing prevented key analysts on certain issues from making fully informed judgments.’

3 The nature of evidence and the new technologies

Evidence takes on two basic forms, that which is a written statement in place of oral transmission, and anything on which something can be recorded. High-tech gadgetry is becoming increasingly useful in storing recorded information digitally. Not only can miniature devices do so with incredible amounts of storage power but they can do so continually 24/7, using very little on-board battery power and with a relatively low degree of risk to humans. Digital documentary evidence that has been used in ad hoc tribunals for instance includes aerial photography, audio and video tapes, maps and sketches of plans, and a variety of digital record formats. 'Such evidence is deemed admissible if it contains information of probative value.'²⁶ Digital evidence especially is prone to tampering however this is the emerging context in which courts now have to operate.

New technologies, which have allowed for covert surveillance to be performed without the permission of a given state, highlight the need for regulation.²⁷ One need only point to the Echelon operation, which was first considered a wild conspiracy, but which was later shown to be a mass surveillance operation by the United States, United Kingdom, Canada, Australia and New Zealand on major European industries. 'It was in short a major scandal of governmental industrial espionage against friendly states.'²⁸ It is not being argued here that new technologies should not be exploited to their maximum potential to prevent or suppress criminality but they presently remain unregulated. So in admitting evidence that has been gathered in another country, national courts need to maintain that the evidence has been gathered within the confines of a given state's domestic law, and not by any other means.²⁹ If we cannot be confident in this, then not only are we making sweeping assumptions about the reach of laws but we are creating a law unto ourselves, to do as we please, as we see fit. When comparing the comprehensive and robust MLA process (although to some seemingly long-winded and bureaucratic), with just-in-time inter-state police cooperation, one can come to the resolution that there is a great divide that needs to be bridged. With reference to police cooperation, it must be said, that better processes with regulations at an inter-state and international level, can only increase the likelihood that cross-border criminals will be brought to justice and tried under the most suitable laws, resulting in a better outcome for all parties concerned.³⁰

In an attempt to bridge that gap the United Nations adopted the Convention

26 Bassiouni, above 1, 656.

27 Bantekas, above 1, 240. 'Due to the nature of modern telecommunications systems, interception frequently does not require technical assistance from other States.'

28 Bassiouni, above 1, 371-373.

29 Bassiouni, above 1, 374. See also, Bantekas, above 1, 255. Interestingly however, '... the Court is prepared to focus on the nature of the evidence rather than the fact that human rights standards have been breached.'

30 David Lanham, *Cross-border Criminal Law* (1997) 44-45.

Against Transnational Organized Crime in 2000 that addressed but did not regulate the question of inter-state law enforcement cooperation.³¹ Articles 26–28 raise the matter of bilateral and multilateral agreements inviting ‘... state parties in accordance with their national legal systems to develop national legislation permitting special investigative techniques’,³² which could then be extended beyond the borders and applicable to law enforcement and intelligence organizations. The articles specifically addressed forms of electronic surveillance and how they might be used in joint investigative operations. For example, although it took several years to agree on, Member States finally ratified a convention which would allow them in appropriate circumstances to intercept communications directly.³³ It should be highlighted that the convention was seen as going soft on data protection and in allowing for dubious practices such as that of cross-border observation, in actual fact, hot pursuit of suspects or fugitives by foreign police officers across borders.³⁴

There is ‘... no evidence [that] exists outside court proceedings.’³⁵ In common law countries facts must be proved beyond a reasonable doubt.³⁶ For a definite conclusion to be sought however, the evidence which has been gathered must also have been collected with the same level of confidence. ‘Implicit in the right to a fair trial is the rejection of evidence obtained in breach of fundamental human rights standards.’³⁷ New technologies and techniques however may not coerce an individual to confessing to a crime, but may apply irregular methods of data collection that in some instances could be considered a type of intimidation.³⁸ A frequent happening in international criminal proceedings is when a prosecutor does not wish to disclose their source of information for reasons of confidentiality,

31 See also, Bantekas, above 1, 236. In Title VI of the Treaty on European Union (TEU) a similar hope was set out, to develop ‘common action among Member States in the fields of police and judicial co-operation in criminal matters.’ The EU has been to some degree successful at achieving these goals, at least insofar as communicating standards, guidelines and protocols to Member States.

32 Bassiouni, above 1, 375. See also, Elia Zureik and Mark B. Salter (eds), *Global Surveillance and Policing: Borders, Security, Identity* (2005).

33 Bantekas, above 1, 239, 259. ‘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.’

34 Ibid 279.

35 Antonio Cassese, *International Criminal Law* (2003) 421.

36 Ibid 425.

37 Bantekas, above 1, 254–255, 284. Proceedings from the *Corpus Juris* Project in Europe stated ‘(1) [e]vidence must be excluded if it was obtained by community or national agents either in violation of the fundamental rights enshrined in the European Convention on Human Rights...’

38 Ibid 245, 246. See, eg, ‘[i]n *R v Terry*, the court also held that the Charter of Rights has no effect on law enforcement officials abroad, and as such does not render illegally obtained evidence inadmissible. ... However, the failure to reject evidence which was obtained not merely in breach of foreign law, but also in violation of international human rights standards ... is lamentable and demonstrates a lack of sensitivity and understanding of the rules operating in other legal systems.’

safety, or other.³⁹ Quite often secret intelligence organizations are not prepared to tell the public how they obtained a particular record or document, and in many instances the evidence provided is still accepted.⁴⁰ Courts are faced with a difficult choice when it is obvious that unlawful means have been used to obtain evidence—excluding the evidence may mean doing away with the reliable information, while admitting it legitimized illicit and irregular modes of investigations.⁴¹

4 Human tracking technologies used for location intelligence

How are authorities able to locate individuals who are suspected of transnational crimes for the purpose of MLA requests and inter-state police cooperation? ‘Mobility is a basic and indispensable human activity that is essential for us to be able to lead independent lives on a daily basis’.⁴² Criminals suspected of a crime—like every other human being—require to move around in public space in order to satisfy basic living requirements. Someone who is moving can be tracked manually or digitally, even if they (or persons harboring criminals) are using cash to pay for their every transaction.⁴³ The information being gathered as a person moves from one place to the next can be considered a type of chronicle or breadcrumb. Today, given the high-tech devices available to law enforcement and intelligence organizations, an electronic chronicle⁴⁴ and electronic breadcrumb⁴⁵ can be gathered, stored, and manipulated for presentation at a later date. To allow oneself to be tracked can be a voluntary act, but in most cases it is imposed by a third party who has some control

39 Bassiouni, above 1, 656–657. ‘The problem, however, is when this evidence is provided by intelligence agencies who do not wish to have their sources disclosed. This issue of confidentiality of sources makes it difficult, if not impossible, to use valuable information.’

40 Antonio Cassese, *International Criminal Law* (2003) 424.

41 Liam Byrne, ‘Admission of Evidence Obtained in Breach of Privacy Laws’ (2007) (78) *Precedent* 21. English, Canadian, American, Australian, Irish and Scottish courts all differ on their positions regarding what constitutes ‘lawful methods’ of data gathering for admittance of evidence in their courts.

42 K. Kayama, I.E. Yairi and S. Igi, ‘Semi-Autonomous Outdoor Mobility Support System for Elderly and Disabled People’ (2003) *International Conference on Intelligent Robots and Systems* 2606.

43 Stephane Leman-Langlois, ‘The Myopic Panopticon: The Social Consequences of Policing through the Lens’ (2003) 13(1) *Policing and Society* 51, 54. ‘The combination of face recognition, motion analysis and sound analysis could become very interesting in the near future.’ Leman-Langlois writes of an ‘omniscient surveillance.’ See also, the notion of ‘überveillance’ in Katina Michael et al, above 15, 7.

44 G. Pingali and R. Jain, ‘Electronic Chronicles: Empowering Individuals, Groups, and Organisations’ (2005) *IEEE International Conference on Multimedia and Expo* 1540.

45 Wherify, *Wireless Location Services* (2005) <<http://www.wherifywireless.com/>> at 29 May 2007.

over the end-user.⁴⁶ Tracking can be obtrusive taking the form of overt surveillance⁴⁷ (ie the individual knows they are being followed), or as in most cases tracking is unobtrusive taking the form of covert surveillance (ie the individual is not aware that they are being tracked).

Today, tracking is possible via a vast array of technologies– from GPS devices, to radio beepers, electronic mail, and even fixed and mobile telephony.⁴⁸ In fact, the use of a mobile phone in most more-developed countries means that a location fix within about 50 meters of the user's handset is possible, just by an individual having their phone on.⁴⁹ Increasingly, mobile phones are also being equipped with GPS chipsets which means that if a mobile device is outdoors, a service provider can perform a position fix within seconds if a request is made by the police.⁵⁰ And it is not only the location position fix that is revealing, even more telling is the continuous, real-time location information that can be gathered by a GPS, including accurate geodetic information, such as longitude and latitude, time and speed.⁵¹ Beyond statistical data, location intelligence 'reveals a great deal about one's preferences, friends, associations, and habits.'⁵² Till now law enforcement agencies

46 R. Cucchiara, C. Grana, and G. Tardini, 'Track-based and Object-based Occlusion for People Tracking Refinement in Indoor Surveillance' (2004) *Proceedings of the ACM 2nd International Workshop on Video Surveillance & Sensor Networks* 81–87. Tracking is critical in the process 'of people motion capture, people behavior control and indoor video surveillance.' See also, Clive Norris, Jade Moran and Gary Armstrong, *Surveillance, Closed Circuit Television and Social Control* (1998).

47 Stephen Green, 'A Plague on the Panopticon: Surveillance and Power in the Global Information Economy' (1999) 2(1) *Information, Communication & Society* 31. 'In the United Kingdom, Newcastle police claim that CCTV has led directly to 2,800 arrests from 1991–9, with 99 per cent of offenders pleading guilty when presented with video evidence ... In contrast to more radical libertarian accounts, the key point here is that not every sacrifice of individual autonomy and 'privacy' is the same as the loss of freedom...'

48 William A. Herbert, 'No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?' (2007) 2(2) *I/S: A Journal of Law and Policy* 410. 'In contemporary American culture, some view the concept of freedom as being manifested in consumerism, with the ubiquitous cell phone as a primary symbol. It is doubtful that most cell phone users are aware that the same technology that grants them this sense of freedom, also results in wireless companies, receiving automatic and continuous updates regarding their location. Physical possession of a cell phone renders an individual vulnerable to location surveillance by government entities...'

49 Katina Michael 'Location-based Services: a Vehicle for IT&T Convergence' in K. Cheng et al (eds), *Advances in e-Engineering and Digital Enterprise Technology* 467. It should be noted that GPS data is not foolproof. Speed miscalculations, location fix inaccuracies, signal dropouts, can all occur due to the physical structures that the GPS passes through, and even to changes in climatic conditions, and the presence of dense foliage.

50 Leman-Langlois, above 43, 46. 'First, there is *deterrence*: overt surveillance aimed primarily at discouraging potential offenders from actually committing crimes. Second, *intelligence gathering*: a police force may be interested in collecting images for their information content, to build files, understand relationships, create chronologies, etc. Third, *evidence*: evidence is information that meets basic legal requirements and is thus admissible in court to support the accusation of a suspect.'

51 Ganz, above 17, 1329. 'One model, which a Law Enforcement Technology Magazine reviewer called a "vehicle tracking system that would make James Bond envious," sells for \$2,396 per unit. Users pay \$59 per month of tracking data used. The product can be attached to a car in thirty seconds and operates anywhere in the United States, Canada and Mexico where cell towers exist.'

52 April A. Otterberg, 'Note: GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment' (2005) 46 *Boston College Law*

have used GPS to investigate murder cases, drug investigations, robbery, public corruption, probation violations and hostage situations.

5 GPS evidence in Court- case law examples in the United States

Although GPS technology has been used in law enforcement since the early 1990s,⁵³ it is only recently that a few cases have been heard regarding the validity of using GPS tracking technology on suspected criminals.⁵⁴ All of the cases presented here are based on case law in the United States. The Fourth Amendment in the United States Constitution is the main source of legislation pertaining to the protection of an individual's right to privacy. 'At present, the United States Supreme Court has not ruled on the applicability of the Fourth Amendment to most recent forms of human tracking technology.'⁵⁵ There have been some landmark cases however, that have pointed towards the requirements for warrants to conduct surveillance activities. Compare for instance the cases *Olmstead v. United States* with *Katz v. United States*. In 1928 the United States Supreme Court determined that the Fourth Amendment did not prohibit the action of eavesdropping using telecommunications networks, while almost forty years later in 1967 the Court held that the FBI's use of a microphone on the roof of a payphone, without a warrant, constituted a violation of the Fourth Amendment.⁵⁶ Still, the Court ruled that using a tracking device to monitor vehicles or objects was not subject to the expectation of a privacy test. For example, a person traveling in a car on a public road from A to B had no reasonable expectation of privacy as he or she was out-n-about in full view of the public.⁵⁷ This decision was again reaffirmed in 1983 in the United States

Review 663.

- 53 Prior to GPS technology, less sophisticated technology was used, known as beepers. Beepers helped locate a vehicle once an event occurred, such as a car door opening or the ignition starting, or movement. Beeper technology could alert police officials to locate the originating position of the vehicle, and thereafter it would be tailgated using traditional visual surveillance means.
- 54 *Olmstead v. United States*, 277 US 438 (1928). *Katz v. United States*, 389 US 347 (1967). *United States v. Knotts*, 460 US 276 (1983). *United States v. Karo*, 468 US 705, 707 (1984). *Kyllo v. United States*, 533 US 27 (2001). *State v. Jackson*, 76 P.3d 217, 220 (Wash 2003). *State v. Peterson*, (Cal 2004). *People v. Lacey*, Indictment No 2463N/02, 2004 WL 1040676 (Nassau, NY County Ct. May 6, 2004), *People v. Gant*, 9 Misc 3d 611 (Westchester, NY County Ct. 2005). See also, Otterberg, above 52, 680. 'Only a few courts have specifically considered whether the monitoring of GPS tracking devices is distinguishable from the monitoring of the beepers in *Knotts* and *Karo*.'
- 55 Herbert, above 48, 417.
- 56 Ibid 418-419, 420. '... by mandating for the first time that the police obtain a court-ordered warrant before engaging in electronic surveillance, the *Katz* decision established a significant judicial check on government agents randomly engaging in such surveillance.' In *Katz* it was also interesting to note a shift in emphasis from protecting a place where someone resides, to protecting the person from government intrusion.
- 57 The definition of a 'public space' and that of a 'private space' has been open to debate in recent times. Is private only the space in which we reside- the four walls of our home when the blinds are down, and the inner lining of our roof? If so what happens when we walk outside our doorstep? Or even more precisely if a vehicle that has a GPS unit attached, enters a garage which is connected to the home?

v. Knotts case when the Supreme Court again ruled ‘that the police did not have to obtain a warrant under the Fourth Amendment before using a radio beeper to monitor the movement and location of a vehicle.’⁵⁸ The Court portrayed beepers as a mere replication of the traditional, manual, police visual surveillance conducted via physically tailing a vehicle.

In *Kyllo v. United States* in 2001 yet another twist to the interpretation of the Fourth Amendment was played out. The Supreme Court declared that protections within the boundaries of the home were only limited to devices that were not in “general public use”.⁵⁹ When one considers the proliferation of mobile telephones many of which are now location-aware or GPS devices that are now found in up-market vehicle models, the United States human tracking possibilities look vast. What may this mean for average citizens wishing to take the law into their own hands and begin to track one another?

At the state and local levels, courts hold differing positions based on their jurisdiction. For the greater part, warrants must be obtained prior to the operation of an electronic device to track an individual. In Washington’s highest court the power of GPS to be more than a tracking device was recognized:

[U]se of GPS tracking devices is a particularly intrusive method of surveillance, making it possible to acquire an enormous amount of personal information about a citizen under circumstances where the individual is unaware that every single vehicle trip taken and the duration of every single stop may be recorded by the government.⁶⁰

However, in the cases *People v. Lacey* and *People v. Gant* the opposite judgment was reached on the same question of warrant requirements for a GPS tracking device on a vehicle.⁶¹ This seemingly contradictory position of the State of Illinois is disturbing especially when one considers the federal constitution in context and the requirement for inter-state agreements in locating criminals or proceeds of crime. Two of the most high profile cases where data was gathered using a GPS and admitted as evidence was in the 1999 *State v. Jackson* and in 2003 *State v. Peterson*. In the Jackson case a judge executed a search warrant on Jackson’s vehicles and residence for ten days, and then subsequently granted two more warrants which were extensions of time for the police to continue with covert surveillance.

Specifically, data showed that on November 6th, Jackson drove his truck to rural Springdale and parked without leaving for forty-five minutes. On November 10th, Jackson made a trip to Vicari and Springdale, two remote sites, where he remained for sixteen minutes and thirty minutes, respectively. The police discovered Valiree’s body in a shallow grave at

58 Herbert, above 48, 420–421.

59 Ibid 424.

60 Ibid 431–432.

61 Ibid.

the Springdale site and promptly arrested Jackson.⁶²

It was the Jackson case which really demonstrated the power of GPS tracking technology to justices all over America, in terms of the privacy implications. Counter-arguments grew however as questions were raised about trusting law enforcement personnel to act appropriately.⁶³ In addition, the question of the right to privacy by a suspected criminal also came to the fore.⁶⁴ It was not until the Peterson case that a judge reaffirmed that GPS location data was acceptable and fundamentally valid as a generic methodology to employ in gathering evidence for a trial.⁶⁵ What these example cases reveal is that the warrant process and admissibility of evidence varies dependent on the jurisdiction. This is magnified when one considers the absence of provisions in an international setting.⁶⁶

More recently the reliability of GPS data has come into question. While the technology can have almost pinpoint accuracy, it does suffer from technological limitations depending on environmental factors. There are a growing band of domestic GPS-related cases in the United States, which have either been lodged by individuals or unions,⁶⁷ challenging companies or employers regarding GPS accuracy and the individual's right to be let alone.⁶⁸ In most of the cases to do with accuracy, GPS speed miscalculations or position fixes are at the heart of the matter—employees have either been fined for speeding in a company vehicle (e.g. truck), or individual consumers have been charged an additional levy for allegedly crossing state boundaries (e.g. car hire).⁶⁹ In October of 2007, there were a few cases reported

62 Tenison Craddock, 'Casenote: The Limitations on Police Regarding GPS Tracking Devices: A Necessary Hindrance?' (2005) 9 *Computer Law Review & Technology Journal* 506-507.

63 Ganz, above 17, 1325. 'Global Positioning System (GPS)-based surveillance systems enable police to cheaply and easily gather intelligence and evidence they would otherwise have to obtain through more costly, cumbersome and risky means such as physical "tails" by pursuing officers. The efficiency gains GPS tracking provides are especially significant because they enable police to extend their operational capability with minimal incremental spending.'

64 Craddock, above 62, 510.

65 Ibid 511.

66 Byrne, above 41, 24. 'Different results can also arise depending on which privacy law is breached and what type of proceeding is in question.'

67 Email from William Herbert to Katina Michael, 10 April 2007. '... The union ... is currently challenging employers who have imposed GPS technology unilaterally on union members.'

68 See, eg, GPSTrackSys, *7th Circuit U.S. Court of Appeals Okays Surreptitious GPS Tracking by Police* (4 February 2007) <<http://gpstrackingsystems.biz/7th-circuit-us-court-of-appeals-okays-surreptitious-gps-tracking-by-police/25/>> at 1 October 2007. 'The fourth amendment protects against unreasonable search and seizure, but the judges ruled that the placement of a GPS tracking device without the suspect's knowledge, does not qualify as a search of his car. This is the first time the seventh circuit has weighed in on this issue, which other circuits have split on. The court equated GPS tracking to police physically following a car, or monitoring safety cameras to follow a car, neither of which amounts to illegal search and seizure.'

69 See, eg, Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving?* FindLaw (23 August 2005) <<http://writ.news.findlaw.com/ramasastry/20050823.html>> at 1 October 2007. 'First, let's look at the Connecticut case. It arose because American Car Rental had a policy of charging its clients \$150 for "excessive wear and tear" to the rental car, each time they drove over 79 miles per hour. American knew exactly when that occurred because its subsidiary, Acme Rental, used GPS

that stipulated that the U.S. government had terminated an employee's contract based on data collected covertly using the GPS chipset in the government-owned mobile handset carried by the employee.⁷⁰ Most of these latter cases have focused on the physical location of the employee—e.g. that employees were claiming financial remuneration for hours not physically worked at the office. But this too is open to misinterpretation—what if the employee worked through his/her lunch break, or took work home with them? We can see by this example how GPS data can reveal only partial truths and cannot be used as the sole piece of evidence. GPS data also has to be stored somewhere—and herein lies its greatest weakness—longitude and latitude position coordinates can be changed on the fly to fabricate evidence (for or against the defendant). Currently only 2 states in the U.S. require a company to let an employee know when they are monitoring them. These cases are only indicative of potential international issues that may arise when GPS is used to track suspects.

6 Human rights v. national security

Privacy advocates and civil libertarians often point to the erosion of human rights through the development and application of novel technologies in the area of law enforcement. It is true, that the new innovations pose legal and political challenges but a balance must be struck between their usage for legitimate purposes such as in the case of fulfilling an MLA request or formalised inter-state police cooperation, and those that may be considered illegal and a breach of citizen privacy.⁷¹ The growing problem is not that these technologies are diffused commercially but the possibility that if they are used for law enforcement purposes, they will eventually find their way into government mandated schemes for the general populous.⁷² In quoting Jacques Ellul, privacy expert David Lyon, brings this notion to light:

“To be sure of apprehending criminals, it is necessary that *everyone* be supervised.” Substitute the word ‘terrorists’ for ‘criminals’ and we have

installed in its cars to monitor renters' speed as they traveled. Whenever GPS reported that the customer drove at least 80mph for more than two minutes at a time, the company charged the customer's credit or debit card \$150.’

70 See, eg, Allen Stern, *Man Fired Thanks to GPS Tracking* (31 August 2007) <<http://www.centernetworks.com/man-fired-thanks-to-gps-tracking>> Center Networks at 1 October 2007. ‘The NY Post reports, “Schools Chancellor Joel Klein yesterday fired a veteran worker whose movements were tracked for five months through the GPS device in his cellphone, leading to charges that he was repeatedly cutting out early.’

71 Richard Abraham, ‘The Right to Privacy and the National Security Debate’ (2007) 78 *Precedent* 33. ‘... Australia lacks an adequate framework for balancing the right to privacy (and human rights in general) against competing rights and interests. ... This is not an argument against maintaining a strong security agency or enacting national security legislation. Instead, it is a call to improve the process by ensuring the effective protection of the very rights they are said to protect.’

72 Otterberg, above 52, 670. ‘...[B]ut what concerns privacy advocates is the tracking of suspects and those who have not yet been convicted of any crime. Privacy advocates draw parallels between such GPS tracking and the Orwellian state—one where the average citizen must live and move about while knowing the government may be watching and scrutinizing the individual's every movement.’

an uncannily accurate description of the world since 9/11.⁷³

For now, sweeping legislative changes that have taken place post-9/11 have coincided with the widespread diffusion and use of human tracking technologies.⁷⁴ The United States has been criticized in particular for their departure from human rights standards; some even going as far as concluding that they have shown disregard for the fundamental principles of international law.⁷⁵ Australia also has received similar backlash by international political commentators:

The new legislation has serious implications for bodily, territorial, communications and information privacy, specifically the *Australian Security Intelligence Organization Legislation Amendment (Terrorism) Act 2003* (Cth); *Anti-Terrorism Act (No. 2) 2005* (Cth); and the *Telecommunications (Interception) Amendment Act 2006* (Cth).⁷⁶

Perhaps what is most disturbing about the new legislation is its lack of clarity in explicitly stating what devices can and cannot be used. For instance, in the Australian Commonwealth Anti-Terrorism Act, a tracking device is defined as: ‘... any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.’⁷⁷ An electronic device could range from a GPS wristwatch to an electronic ultra high frequency (UHF) bracelet to an invasive radio-frequency identification (RFID) implant. In the United States, the phrase “electronic instrument” is used instead.⁷⁸ While legislation is drafted with the knowledge that technology changes occur at a fast pace, there is an increasing requirement for clarity, especially as embedded ‘beneath the skin’ technologies rise to the fore. Chip implants clearly violate the individual’s private space, ie, they penetrate the body. For civil libertarians the question is who decides whether someone is a suspect to a crime? And if someone is innocent until proven guilty then how can a government justify the use of tracking devices upon one of its citizens? The argument is that technologies like GPS tracking technology are manifold more powerful than police visual surveillance and that high-tech devices allow police to monitor people

73 David Lyon, ‘Sorting for Suspects’ (2004) 70 *Arena Magazine* 26.

74 Alan Davidson, ‘Electronic surveillance regulations’ (2004) 24(9) *Proctor* 31. ‘The [Patriot] Act authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored email or communication records.’

75 Bantekas, above 1, 18–19.

76 Abraham, above 67, 32.

77 Anti-Terrorism Act (No. 2) 2005 (Cth) s100.1(1)

78 Robert Chalmers, ‘Orwell or All Well? The Rise of Surveillance Culture’ (2005) 30(6) *AltLJ* 260. ‘At the COAG meeting, the Commonwealth and States agreed on enhanced tracking (perhaps even pre-crime electronic bracelets for people subject to control orders) and other extended law enforcement powers, subject to extended sunset provisions.’ See also, Europa, ‘Ethical aspects of ICT implants in the human body: opinion presented to the Commission by the European Group on Ethics’ (2005) <<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/97&format=HTML&aged=0&language=EN&guiLanguage=de>> at 29 April 2007.

‘...for a much longer period of time, with much less chance of detection.’⁷⁹

7 Recommendations

There are many recommendations that can be made towards the use of human tracking technologies in inter-state police-to-police cooperation. However, first there must be an acknowledgment that there is a via media in ‘protecting citizens’ reasonable expectations of privacy and permitting law enforcement officials to do their job.’⁸⁰ The via media is the radical middle, the radical centre, centrism, and the third way philosophy.⁸¹ When one considers the extreme polar arguments they are inherently flawed. Compare for instance the staunch position of some civil libertarians who see all forms of surveillance in all circumstance as a degradation of human rights versus some secret police organizations who wish to by-pass all legal procedures. There is surely a middle position with a workable solution. Parts of the solution may include the constitution of uniform procedures to be set up and adopted for inter-state police cooperation, just as there currently are treaties for MLA requests, police self-regulation to be more explicit about the acceptable use of human tracking technologies with embedded prohibitive clauses, and the mandate for warrants and court orders to be obtained prior to the implementation and monitoring of an individual.⁸² A more difficult goal to achieve is the alignment of state and federal laws of countries pertaining to human tracking technologies and their limitations in terms of admissible evidence in a trial.⁸³ This will come with time as more and more international cases are heard on the matter of location intelligence being used in a court of law to help in the conviction of a criminal.⁸⁴ These recommendations are not merely meant to solve band-aid ‘jurisdictional problems’ when police track individuals across state lines but are recommendations towards a common protocol.⁸⁵ Perhaps some of the more pressing questions that

79 Otterberg, above 52, 697-698. ‘The resultant lengthy, detailed record of one’s location then provides a comprehensive picture of one’s life. Location information reveals everything from daily habits like stopping at the same coffee shop on the way to work, to associations with other people, to visits to locales that reveal much more about a person’s particular characteristics, affiliations or beliefs—such as a gay bar, a certain church, synagogue, or mosque; a strip club; or various political and civic organizations.’

80 Simon Bronitt and Henry Mares, ‘Privacy in the Investigative Process: Striking a Balance?’ (2002) 14(3) *LegalDate* 2. See also, Bantekas, above 1, 75. ‘In the preamble [of the Council of Europe Convention on Cybercrime] reference is made to the need to maintain a balance between the interests of law enforcement and respect for fundamental rights.’ See also, Colin J. Bennett and Rebecca Grant (eds), *Visions of Privacy: Police Choices for the Digital Age* (1999).

81 See also, Lanham, above 30, 55.

82 Ganz, above 17, 1325-1326. ‘While the use of GPS tracking devices grows among law enforcement, federal law remains largely undefined regarding the need to obtain warrants before their deployment. State law presents a similarly mixed picture...’

83 Ibid. ‘The federal-state split is a function of differing constitutional conceptions of personal privacy.’

84 Bassiouni, above 1, 682. ‘The need to harmonize the criminal international criminal justice system and national criminal justice systems’ is a matter that is relevant to human tracking technology as well.

85 Otterberg, above 52, 679.

courts will face in the shorter term are: when is it appropriate to use particular types of electronic devices for surveillance, for how long, and to monitor what type of activity.⁸⁶ These questions become even more complicated when we consider them across borders.⁸⁷

⁸⁶ Chalmers, above 78, 260.

⁸⁷ Malcolm Anderson and Joanna Apap, *Police and Justice Co-operation and the New European Borders* (2002).

18

ePassport security under the microscope

Matthew Sirotich

Honours Candidate, School of Information Systems and Technology, University of Wollongong

Abstract

This paper focuses on ePassport security which utilizes RFID chip technology. ePassports are increasingly being used by governments to enhance the border entry and exit process. The paper briefly describes the nature of RFID technology and its characteristics pertaining to different aspects of security. The approach taken in this study is two-fold: experimental in the first instance, followed by a proof of concept (POC). The experimental study uses metrics to draw conclusions pertaining to the security, safety and privacy viability of the ePassport. Conclusions drawn from the experimental work are used to inform a proof of concept (POC) which provides one possible solution to eradicate the current issues related to the existing ePassport implementation. The proposed ePassport system is then compared to the existing ePassport using the defined metrics to determine which system provides the end user with the most privacy and security. The basic premise for this study is that if new technology is instituted to increase state security, then it should not be plagued with problems which would only increase national security concerns.

Keywords: ePassport, radio-frequency identification, security

1 Introduction

A radio frequency identification (RFID) tag is a “tiny, inexpensive chip that transmits a uniquely identifying number over a short distance to a reading device, and thereby permits rapid, automated tracking of objects” (Jules, 2005a p. 1). Fundamentally it is a device which responds to queries from readers with a unique identification (UID) number. This paper deals exclusively with passive tags which do not have their own power source and gain their power from reader interrogations. As the medium for interaction is radio waves, the tag must be relatively close to the reader because the intensity of the radio waves (and all other electromagnetic waves) obeys the inverse square law. This law states that as the distance increases, the intensity (I) decreases inversely by the square of the distance (d) (Centre, unknown).

I.e. $I = \frac{1}{d^2}$

Once a message has been transported from the reader to the tag via electromagnetic waves the tag will power itself through inductive conductance and reply with its UID and optional information such as a Universal Product Code or some predefined value. The reader will now capture this information and transmit it to a back-end system. When this information is received it will be processed and possibly shaped into structured queries (commands that search, alter etc a database) that may be used to update databases (Wamba, 2006).

RFID is a wireless technology and hence interactions are not necessarily observed meaning that there is the potential for transactions to occur in stealth. With attributes like this, security concerns regarding tracking and much more are coming into question (Want, 2004).

2 The cornerstones of security

Before this paper can proceed an understanding of what is implied by security must be defined. Security is the provision of confidentiality, integrity, and availability (Bishop, 2002).

- *Confidentiality* is the ability to keep a secret a secret, it is the provision to ensure your private effects remain under your control. Access control mechanisms help provide a user with confidentiality, such access control mechanisms are passwords, tokens, biometrics, cryptography etc.
- *Integrity* is the assurance that data is correct and not malformed, i.e. it represents wholly and truthfully the information it was intended to or originally documented to. Two techniques exist to provide integrity which are prevention (which ensure only authorized people edit data) and detection (the act of determining when data has been altered such as a checksum).
- *Availability* is the assurance that the data is accessible by authorized parties at all times.

Cryptographic operations, data hashing and pseudo random number generation are normally used to provide this security. A typical example of data hashing is the MD5 scheme which “takes as input a message of arbitrary length and produces as output a 128-bit “fingerprint” or “message digest” of the input” (Abzug, 1991). In the RFID context it is however currently impossible (Brainard, 2004) for a passive tag to carry out these calculations as they do not have their own power source and gain their power from reader interrogations. As this is the case other techniques such as embedded checksums must be applied to these RFID tags to ensure their security.

3 RFID security approaches

Molnar et al (2005) take into consideration that the challenge is to provide privacy protection without raising tag production and running costs. With this in mind they developed the theory of privacy for RFID through *trusted* computing. This proof of concept explains that tags will be developed to be used with dedicated readers that contain a trusted platform module (TPM) which is also known as a trustworthy reader. This ensures that a tag’s privacy is respected and hence data that is not meant to be read by the reader is not read. The threat model they define is that the reader can be compromised, but the TPM cannot as it is a tamper-resistant hardware module. The reader is split into 3 distinct portions, the:

- Reader Core – is the radio interface, basically an RFID reader as we know them today
- Policy Engine – software that controls reading to ensure it is preserving privacy
- Consumer Agent – enables users and organizations to interrogate the reader to ensure it is conforming to privacy standards (a monitoring tool).

When scanning of a tag is to occur, the policy engine receives a request for read secrets, this is then passed to the TPM which determines if the reader core is valid. If all checks are passed the data is given to the trusted root and the policy engine is executed (Molnar, 2005). Yet the authors seem to cast doubt over their own proof of concept. While they state that “these ideas could be implemented today,” they go on to admit that “significant engineering challenges remain” before the product can be shipped” (Molnar, 2005, p. 3). Seeing as this implementation of a TPM is yet to be built and tested and a growing distrust for trusted computing is evolving, it can be assumed that this technology is under scrutiny by community groups. Schoen (n.d.) is of the belief that *trusted computing* is not the answer as it delivers users new risks of anti-competitive and anti-consumer behaviour. Another risk is that manufacturers of trusted computing hardware may produce their products with ‘defects’ (Schoen, n.d.).

Another interesting security implementation for RFID tags that again places the trust in the hands of the reader is the technical proposal of Jules (2005) which

describes ‘the privacy bit’. In this technical proposal a bit called the *privacy bit* is added to the tags memory which tells readers if the tag is in private or public mode. The theory relies solely on the readers being trustworthy and that restrictions are placed on the firmware or software to ensure the readers respect tag privacy (Jules, 2005a). As stated, this theory places the reliance of trust on the reader, what if rogue readers were used such as those described by Newitz (2006)? Researchers such as Westhues (2003) can devise their own readers, and it can be assumed that unscrupulous people creating their own readers will not ensure that their devices are respectful of tag privacy. Jules (2005) admits that the technology has not yet been released and also admits that standards bodies have not accepted the idea, however Jules is relying on developers to realize the problems of consumer privacy and maybe then his solution may have a chance (Jules, 2005a).

The *kill command* is another technical approach which finally puts the onus on the tag to be trustworthy. The tag has a built-in command such that when the tag is authenticated to a reader, the reader can send the kill command to the tag and the tag will self destruct rendering itself unusable. The issue however is that no confirmation is given to whether the command was successful or if the command even reached the reader. Karjoth et al. (2005) have presented a revised version where visual confirmation can be observed as the kill command is a manual process of removing a pull tab which is part of the antenna. When this tab is removed the tag can no longer send or receive messages, nor power itself and hence is rendered useless (Karjoth, 2005). While this option is attractive and appears to be the most viable and most secure, it does not suit many environments as the user may wish for the tag to operate for their own purposes. This kill command is however currently enabled on RFID tags in circulation and is the first of the listed security technologies to be used by consumers and businesses.

Finally blocker tags present a new perspective, instead of relying on encryption and trust, deception is used. This system allows a tag to generate a set of 2k UID’s which floods the reader with responses and leave it up to the reader to determine which UID is the real one (Brainard, 2004). Whilst this approach is very promising and has been shown to work in field studies and does not require changes to current RFID systems, it can be categorised as malicious because the flooding process can be described as a Denial-of-Service (DOS) attack (Jules, 2005a).

4 Established RFID security issues

As shown in section 3 there are avenues that can be followed to secure RFID systems, however, each approach has its own respective limitations. This downside means that the RFID security technique is flawed, as RFID systems cannot provide any guarantees on confidentiality, integrity and availability as is explained below:

- Access is not always authenticated. Westhues’s (2003) device enables him to read RFID tags in passing and gather the data off the tag.

- Integrity cannot always be preserved. Integrity is provided via detection and prevention. From the security approaches in section 3, it is obvious that none implement either of these,
- Availability can be compromised. As detailed by Jules (2005a) denial-of-service attacks can cause the reader to reset.

The major threats posed by RFID systems in humancentric applications are *tracking* (the act of following a tags movements based upon its UID response to interrogations) and *inventorying* (allowing a user to identify object(s) being carried by another person) (Jules, 2006). Whilst this threat seems to contradict the reason RFID tags exist (to track and find objects), in humancentric applications the user needs to have the ability to be anonymous. Inevitably these shortcomings result in personal security threats as people can be followed based upon the UID numbers emitted by their personal effects. More seriously alarming though, personal information can be edited and read by anyone with the technology and the know-how (Westhues, 2003).

5 RFID in ePassports and possible security attacks

An ePassport is just like an existing passport however it has an RFID tag inserted in it which essentially holds the same information that is stored on the biographical page of the passport.

The same information as a passport's data page- passport holder's name, nationality, gender, date of birth, and a digitized photo. It will also store the passport number, issue date, expiration date, and type of passport (Department, 2005).

The RFID chip is simply a second data source which is used to verify the printed data on the passport and hence identify the bona-fide holder with increased confidence. The rationale behind the ePassport is to provide better protection against misuse and tampering, reduce identify fraud, enhance border protection and provide fast and efficient passport checks (Trade, n.d.). Civil libertarian groups especially however question the motivation for the rapid implementation of the ePassport.

To use an ePassport, a user opens their passport to the biographical page and presents it to the identification machine. This machine will read the specially prepared area called the *machine readable zone* (MRZ) which provides the identification machine with the 'key' to decrypt the public key (PKI) ciphertext which safeguards the data. Once this step is complete, a check occurs to ensure the data on the RFID matches the data on the passport's biographical page (Trade, n.d.; Launch of ePassport, 2005). The US state department has taken an experimental approach to proving the security of their ePassports (which follow the same ICACO design standards as Australia's), however how secure this system is has been kept a secret. Extensive testing has occurred however the department is not releasing their findings (Gonsalves, 2005).

The most deep-rooted problem with RFID passports is not to do with the technology itself, but the policies which govern the technology in the passport domain. Coffee (2006) explains that “[a] passport with a failed e-chip remains a valid travel document”. The reason this must be emphasised is because RSA laboratories report that an RFID chip can be deactivated with nothing more than a microwave (Laboratories, n.d.). Furthermore RFID’s utilize the radio wave medium to communicate, hence any transmission can be observed by a rogue reader within the right range. Eavesdropping is a major security issue for RFID not just because it is hard to stop, but harder still to detect (Juels, 2005b). Whilst the government has employed Faraday cages into its ePassport design, it is not inconceivable that an ePassport could become even a fraction open when being carried in a bag or purse hence allowing it to become compromised (Lamb, 2006). On the successful capturing of a signal through eavesdropping, the perpetrator is given the options of:

1. using the signal in a replay attack: send the same signal again at a convenient time such as when posing as the victim (Answers.com, n.d.) or;
2. an offline attack: where the signal is taken and interrogated to possibly break the encryption etc (Chuvakin, 2004).

Moses (2006) has also documented claims by Laurie, which reveal that it is possible to skim peoples’ information from their ePassport. This is contradictory to the statements made by the Department of Foreign Affairs and Trade spokeswoman that one cannot “compromise the security of Australia’s ePassport.”. The department states that there is no way to read the RFID tag without first obtaining the key which is printed in the machine readable zone on the biographical page of the passport. However this information is simply a mixture of the date of birth, expiry date of the passport and the passport number which Laurie explains can be determined through sources such as online airline bookings (Moses, 2006). Due to this evidence it is clear that another method must be constructed which allows this technology to provide privacy and security for its users.

A reader can be set to continuously scan for ePassports, when one of interest is found the user can follow the RF waves much like following an electronic beacon. Critics such as Munro (2007) believe that the new ePassport systems could be used to track a user quite simply if readers are placed in the right position. When considering Gonsalves (2005) claims that the RFID tags in passports can actually be read from up to 30 feet, it is no wonder that conspiracy theories surrounding the potential for governments to track passport holders are on the increase. These notions are highlighted by the likes of Lamb (2006) who state that “[t]here’s clearly something else that they [the government] have in mind here, and we believe that they want the ability to track people without their knowledge.” These claims are continuously given more force when it is considered that the US government continued with the deployment of ePassports even after receiving 98% negative feedback from the public regarding the proposal (Lamb, 2006). Whilst these claims

are not supported by current technical evidence, they do carry some weight.

Finally, the ePassport places all of the user's personal information along with a digital photo onto an RFID chip. It is all there for the taking, in one *basket* and plans are in progress to use the same basket for even more. The ePassport was designed conforming to guidelines provided by the (International Civil Aviation Organisation (ICAO)), one of the design aims for the ePassport is to "[provide] a path to the use of ePassports to facilitate biometric or e-commerce applications" (Kaliski, 2005). This increases the exposure of the ePassport and increases the risk of skimming and tracking. All in all it is just giving unscrupulous people more opportunities to steal your identity. All the user's information is in a single location (the RFID chip) for the taking. If someone does break into the chip they will have all the centrally stored personal information and the owner would not even know it. Whilst this theft of information could occur in a more clandestine fashion, simply by stealing the passport and copying the information from the biographical page, the difference is that someone may notice their passport physically missing, however they would never know if someone remotely had broken into their chip and stolen their data.

6 Assessment of RFID's in ePassports

Before a new, more secure implementation of an ePassport is possible, it is a necessity to first assess the current technology being utilised. The rationale behind these experiments is to create metrics by which to measure and assess security in RFID which can then be reflected in an ePassport system. Not only are these experiments paramount in assessing the current implementation of RFID tags in ePassports, they are also central in creating a revised implementation of the ePassport which will eliminate predecessor faults. The completion of each forthcoming experiment will culminate in a value which will be either 'breached' or 'resisted breach' as defined by the unit of measurement.

6.1 The Experiments

The following experiments were carried out with either Standard Apparatus 1 or Standard Apparatus 2.

6.1.1 Standard Apparatus 1

The apparatus used was a Motorola/Symbol XR400 RFID reader connected to 2 antennas configured in a non portal configuration. This system had an adjustable reading range of approximately 3 meters to 1 centimetre. The antennas were facing opposite directions and separated by a distance of 2 meters. The apparatus was configured to scan continuously for Class 0 and Gen2 tags. Whilst this system had an excellent read range, and was highly configurable with regards to scan frequencies, distances and types, it did not have the capabilities to read the actual data stored on the tag.

6.1.2 Standard Apparatus 2

The apparatus used was a BlackBerry handheld RF scanner which was configured to scan for ISO, Milfare, I-code and other protocols. This scanner had an extremely limited range of less than 5 centimeters and hence was limited in its usefulness, however it did allow for the data in tags to be read and stored.

6.2 Experiment 1- Injection attack on RFID

Aim: To determine the possibility of malforming database queries to cause detrimental database functions.

Hypothesis: *Injection attacks* are malformed database queries which trick the database into doing something otherwise illegal. This could be actions such as editing a certain entry or dropping an entire table. This form of attack has occurred time and time again over the internet in which interactive forms retrieve user data (which may be malformed) and edit a central database according to the data retrieved (Buehrer, 2005; Orso, 2005). It is to be assumed then that injection attacks are possible for RFID systems as the only object changing in the two instances is the medium upon which information is delivered to the back-end system (http to wireless communications).

Method: The ‘Standard Apparatus 2’ was used to read a set of 3 RFID tags. The tags ID and data were as follows:

ID	Data
1111111111AAAAAAAAAAAA1439	Item1
1111111111AAAAAAAAAAAA1438	Item2;Drop Table Data_table;
1111111111AAAAAAAAAAAA1440	Item3

An SQL server is constructed with a table named ‘Data_table’ consisting of a single column called data. This SQL server then interfaces with a simple program which extracts the data held in the ‘docked’ scanner and constructs SQL queries which insert the scanned data into the database such as “INSERT INTO Data_table VALUES(“EXTRACTED DATA FROM SCANNER”);”.

Results: After the program updates the database with the first data element in the docked scanner the database reflects:

Data_table

data
Item1

After the second data element is processed, the database reflects: ‘ERROR, NO SUCH TABLE’

After the third and final data element is processed, the database reflects: ‘ERROR, NO SUCH TABLE’.

Security breach: Breached.

Conclusion: It has been shown that the malformed tag data deleted all items and the entire database. After the second tag was added an error was reported stating that the table specified 'Data_table' did not exist. This hence proves the hypothesis correct and it can be stated that an Injection attack can occur on a database system if the strings used to create the structured query are not parsed correctly.

6.3 Experiment 2- Blocking a reader

6.3.1 Part A - Faraday cage

Aim: To create a more secure Faraday cage in which to encase the ePassport to address the current Faraday cage faults found by Flexills (2006).

Hypothesis: Currently a Faraday cage exists in the cover of the ePassport but as Flexills (2006) pointed out, if the ePassport is thrown into a bag or purse and opens only slightly, it is possible to read the passport. To overcome this, a purse like design which is lined with a foil will alleviate the issues and prevent reads from occurring unless the passport is removed from the purse.

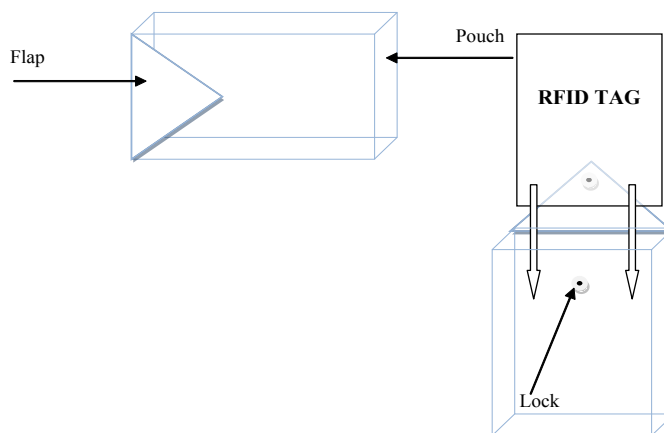


Figure 1- A Faraday Cage

Method: The Standard Apparatus 1 is used to firstly read a tag to create a control. Alfoil was then used to fashion the below pouch allowing enough space in the pouch to snugly fit the RFID tag.

Once complete the tag is placed into the pouch as shown and the flap locked into place. The Standard Apparatus 1 is then set to continuously scan for the tag. The flap is then opened and the scanning is allowed to continue. Finally remove the RFID tag completely from the pouch and ensure the tag can still be read.

Results: The control tag returns its tag ID when it is not encased in the pouch but when placed inside the pouch with the flap shut the tag ceases to respond

at all. Even when the flap is opened, the tag still does not respond. When the tag is completely removed from the pouch the tag can be read and replies with the correct tag ID.

Security Breach: Not applicable.

Conclusions: The new pouch enclosure design is by far a more secure method to house an ePassport. The experiment proves that the tag cannot be read when it is housed in the pouch, even if the flap is not secured. The current ePassport Faraday enclosure is susceptible to reads when the ePassport is partially open hence suggesting that the proposed enclosure will provide a higher degree of security.

6.3.2 Part B - External wave injection

Aim: To disrupt the reading of a tag for a short amount of time enabling a tag to pass by a reader unnoticed.

Hypothesis: An RFID tag uses radio waves as its transmission media, hence some device producing radio waves may disturb the transmission from the tag to the reader or visa versa (Australia, 2007). This phenomenon will prevent the tag from being read by a reader by either invoking destructive interference which degrades the message such that sense cannot be made from it, or abolishes the message all together. This occurrence will therefore enable the RFID tag to pass by the reader unnoticed.

Method: Apparatus 1 is set up along with a Sony Ericsson S700i (GSM with 900MHZ radio transmission). The Sony Ericsson is placed 5 cm behind a tag (class 0). The reader is then set to continuously scan the tag, which is hence read continuously. The phone is then set to initiate a phone call (emit a large amount of wave interference). The read rate is then assessed and then compared to the rate recorded when the phone call is terminated.

Results:

Condition	Read rate
Before phone is introduced to system	Approximately 1 read per second
Phone introduced, call not initiated	Approximately 1 read per second
Call initiated	0 reads per second

Security breach: Breached.

Conclusion: A large amount of wave injection into an RFID system can disrupt reader interrogations causing tags to pass by unnoticed. This application could be used to allow a user to pass by in stealth or even temporarily disable the chip in the ePassport, reverting it to a basic passport.

6.4 Experiment 3- Skimming an RFID tag

Aim: To determine the possibility of tracking a user and skimming information off their RFID enabled objects in a small scale example.

Hypothesis: Well-placed readers will provide enough information to allow inference to take place to a high degree of confidence. These readers will not only enable the tracking of a user, but also provide information about the RFID enabled items being carried. This occurrence is highly intrusive and provides the system owners the ability to profile and keep tabs on the user's tag.

Method: The Standard Apparatus 1 is used but the antenna configuration is modified to better model a real life implementation. Firstly 2 more antennas are added to the reader and all readers read ranges are reduced to 35% (this approximately reduces the read distance to 1.05 meters). The antennas are now spaced out around a room such that the antennas read zones do not cross over and allow dead zones (areas where no reader is monitoring the space) to occur to represent larger distances between read points. The antennas themselves represent buildings or public places. At selected antennas, tags are positioned to represent items that a user may wish to take. A user is now given a tag with a recorded tag ID and encouraged to move around the room at their own discretion and pick up any tags (items) as they please. As the user now moves around the room with their unique tag ID they are tracked via the antennas, each time a user enters an antennas zone, a log is formed with a time stamp. This log reflects the time the tag ID was interrogated and the tag ID itself. As the user picks up tags (items) and makes the transition to another zone, it will be evident that they are carrying the tag as it will show up in a new zone with their unique tag ID.

Results: Table 1 below represents the recorded events. The antennas were named North, East, South and West for obvious reasons.

The table shows a user (1111111111AAAAAAAAAAAA1437) started at the Northern area. Two items were also positioned at the South and East areas. The user progresses to the Eastern area and continues to slowly move into the southern areas. Here they pick up an item (1111111111AAAAAAAAAAAA1436) and continue moving with this item into the Eastern area.

Security breach: Breached.

Conclusion: It is possible to track a user, skim for information regarding what they are carrying and hence profile the user. The occurrence of this security breach allows the RFID infrastructure owners to become ever more pervasive in the user's life. It allows the surveiller to know when a user carries out an act, when they purchase something, when they are at a certain location and so much more. This breach allows for the formation of a 'Ralker' (RFID Stalker) which under other mediums is outlawed and only lawfully granted to governments under certain circumstances.

Table 1- Experiment 3 results

TAG ID	TIME STAMP	TAG TYPE	ANTENNA
1111111111AAAAAAAAAAAA1437	09:07PM 2/10/07	CLASS 0	NORTH
1111111111AAAAAAAAAAAA1436	09:07PM 2/10/07	CLASS 0	SOUTH
1111111111AAAAAAAAAAAA1431	09:07PM 2/10/07	CLASS 0	WEST
1111111111AAAAAAAAAAAA1437	09:08PM 2/10/07	CLASS 0	EAST
1111111111AAAAAAAAAAAA1437	09:08PM 2/10/07	CLASS 0	SOUTH
1111111111AAAAAAAAAAAA1437	09:08PM 2/10/07	CLASS 0	EAST
1111111111AAAAAAAAAAAA1436	09:09PM 2/10/07	CLASS 0	EAST

6.5 Experiment 4- Killing an RFID tag

Aim: To destroy an RFID tag such that it will no longer respond to reader interrogations.

Hypothesis: An RFID tag contains a small circuit board, like all circuit boards too much voltage or current will cause the board to overheat. As an RFID tag gathers its electricity from electro magnetic frequency (EMF) radiation, it is assumed that a large burst of EMF radiation will cause the circuit board to overheat.

Method: An RFID tag is firstly scanned to ensure that it is in working order. The tag is then placed into a microwave and set on high for 10 seconds. The tag is then removed from the microwave and scanned to determine if the tag is still usable.

Results: The RFID tag read correctly before entering the microwave, however after 10 seconds in the microwave the RFID tag failed to respond to reader interrogations. Whilst in the microwave a bright glow was recorded coming out of the RFID tag, this was assumed to be the circuit board of the RFID tag *frying*.

Security breach: Breached.

Conclusion: The microwave appliance emits short 2.5 GHz waves called microwaves when it is turned on. These high frequency waves caused an increased voltage to flow inside the induction coil into the circuit board. This hence proved that if a large burst of EMF waves comes into contact with an RFID tag it can be destroyed.

6.6 Experiment 5- Flooding a reader

Aim: To flood a reader with so many requests, the reader either shuts down or

allows tags to pass by its reading range unnoticed.

Hypothesis: It is possible to flood a reader, but not overly practical as the amount of tags required will not be easily concealable or manageable.

Method: Countless class 0 tags are placed within a single antenna's read range. One tag with a known ID is kept out of the read range to test if it can pass by unnoticed. The reader is then turned on and the known tag is moved into the read range and then removed from the read range. The known ID is then searched for to determine if it has moved into the system unnoticed.

Results: A flood could not be created within the laboratory as not enough tags were available to cause the reader to read incorrectly. This was shown by the tag appearing each time it was introduced into the system and then removed.

Security breach: Resisted breach.

Conclusion: A flood attack on a reader is theoretically possible, however may not practically be possible if a read range was reduced to 10 cm. There would not be enough room to position enough tags to cause the flood to occur (for a summary of results from each experiment, see table 2 below).

Table 2- Summary of experiments and meta-analysis and their effects on ePassports

Security Breach	Does it impede on the privacy and security meant to be provided by the ePassport?
Skimming	A user could be followed and profiled, a smart bomb could be created if commonalities in data were found.
Injection attack	A database could be destroyed hence rendering the ePassport system useless.
Faraday cage failing	The failing Faraday cage in the current ePassport allows for rogue reading in stealth.
Killing a tag	A tag can be killed and hence reduce an ePassport back into a paper-based passport. Hence no added security.
Copying a tag and mimicking	An ePassport could be copied and the encryption taken home to be used in an offline attack to decrypt the data.

6.7 Compare experimental results with the work of Wethues

The work of Wethues (2003) has to be assessed in a meta analysis as the technical requirements needed to build his device are beyond the scope of this study. To provide credibility to Westhues's findings as this study could not test his creation, Newitz's (2006) article is cited as it describes the device in question. Wethues (2003) has developed a device which is capable of reading an RFID tag, copying the unique ID emitted by that device and then replaying the captured ID to a reader. Simply put, Westhues has created a 'replay attack' over the RFID medium. The device has a small read range and requires the user to almost brush past the tag they wish to

copy, however if the device is set up near a read point, the read distance is magnified enormously as the card is being 'excited' by another reader. This phenomenon allows the device to read tags from behind a wall or over a distance (Westhues, 2003).

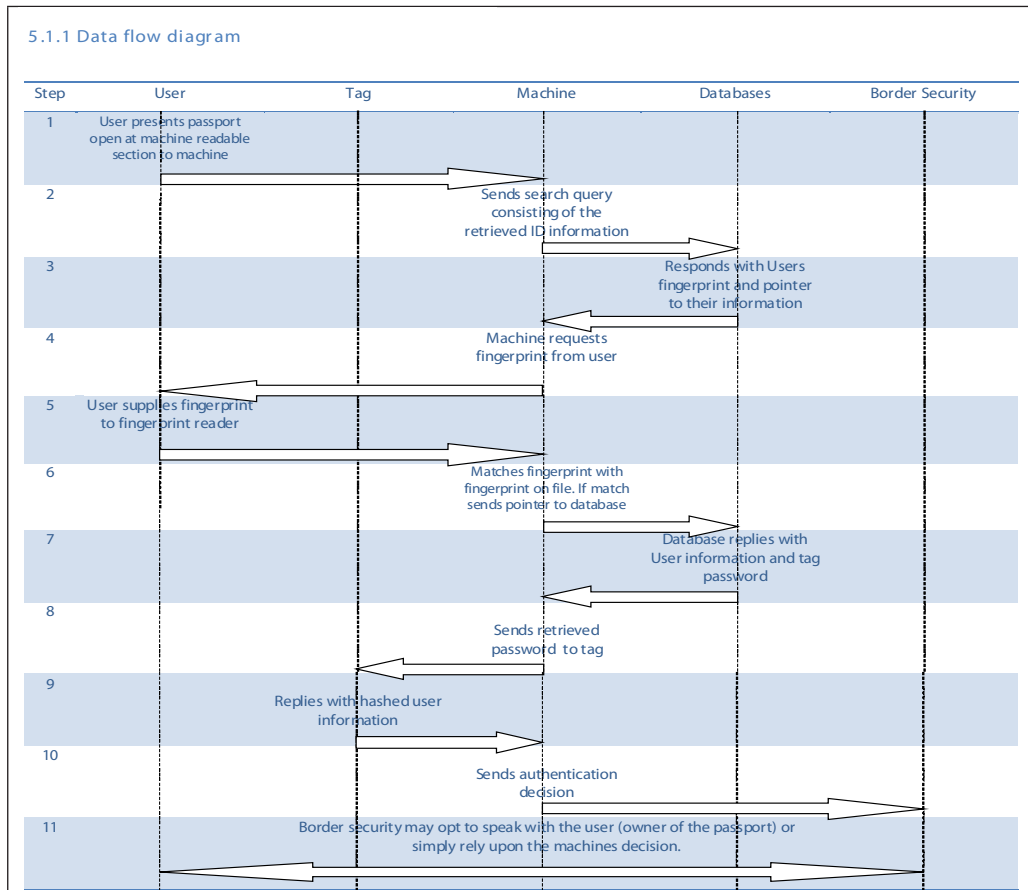
To provide the much needed credibility to these claims, Newitz (2006) describes an encounter she has with Westhues. The author describes watching Westhues walk past an Internet security company, CEO James Van Bokkelen with a concealed antenna in the palm of his hand. Westhues returns to Newitz and plugs his device (via USB) into this laptop to determine if a signal was correctly recorded. Convinced that a successful read occurred, Westhues proceeds into the office building and sets his device to 'mimic' mode and waves his antenna in front of the proximity reader. Newitz (2006) concluded this device to be a complete success because the door in front of them unlocked and opened. This occurrence reinforces that RFID tags are not secure and can be copied at will. Furthermore, if this device was brought into the ePassport domain, the device owner could walk through an international airport stealing people's passport details in stealth. They could then return home and begin cracking the encryption hiding the data sets. With this information they can begin to commit fraud and identity theft.

It has been shown that the current implementation of the ePassport was not well-thought out and allows for unscrupulous people to steal personal information and misuse this information. Through the meta analysis it has been shown that it is possible to steal information using an RFID device and record the data. This data could then be used in an offline attack as described by Sterling (2006) and Lettice (2007). The added security that the ePassport is intended to provide is shown to be non substantial but also shown to reduce the data security of its users. With this knowledge it is assumable that another implementation must be sort after such that the intended benefits can actually be achieved.

7 Proof of Concept

This paper has identified a number of shortcomings with the current ePassport technology. The proof of concept below is aimed at developing an ePassport which is more secure than the existing one by:

- Removing the ability to skim and track the ePassport by implementing a user verification system for the tag.
- Removing the flimsy encryption system and replacing it with a multi-tiered security system without a single point of failure.
- Providing a better implementation of the Faraday cage to deter rogue scanning.

Figure 2- Message Flow Diagram

7.1 Steps Explained

Step 1: The user opens their passport to the machine readable zone and places it on the read point of the machine. The machine will then scan the passport to retrieve the data from the MRZ.

Step 2: The data that has been obtained from the passport is now used to construct a database query. This data is simply date of birth, first name, last name etc (information that is already contained on the passport). The query is then issued to a database and a return is expected. This is the first layer of security, as a query that retrieves no records means that the identity this person is attempting to masquerade does not exist.

Step 3: If a match is found in the database, the users 'fileprint' (Khanna, 2004) and a pointer to the user's information in the second database is returned.

Step 4: The machine requests that the user place their fingerprint over the fingerprint reader so that a 'searchprint' (Khanna, 2004) can be obtained.

Step 5: User supplies their own fingerprint ('searchprint') as the machine requested.

Step 6: The 'searchprint' and 'fileprint' are now compared, if a positive match is

found then the pointer to the next database will then and only then be followed. If the pointer is to be followed, the database will be queried with the pointer to directly access the information required. This is the second step of security which proves that the identity claimed belongs to that physical person through biometrics.

Step 7: The database replies with the user's information (which is everything that would be printed on the passport such as date of birth, names, etc.) along with a tag password. This tag password exists in a 1-to-1 relationship by which only one password exists for each unique tag.

Step 8: The retrieved password is issued to the tag. The tag will only respond with its information when it receives the correct password. This system provides a third step in security to ensure that the RFID chip within the passport is the correct chip for this identity, if the correct password was not encountered the chip would not respond. As a further security precaution, incorrect passwords could be sent at random to the tag to ensure the tag is not compromised and programmed to respond to anything. This password system is adapted from the *kill-tag* system which when the correct password is received the tag calls its kill function and disables itself. However this adaptation replaces the kill function with a reply function and removes the standard reply function entirely as this proposed system never intends for the tag to reply under any other circumstances.

Step 9: If the correct password was encountered, the response is a hash string which is an ordered concatenation of the user's information and password which is then put through the MD5 hashing scheme.

Step 10: The machine will now hash the database retrieved user information and compare the hash output to that obtained from the passport. This is the fourth step in security which ensures that the information on the tag does actually represent the bona-fide user. The reason the tag stores a hashed version rather than plain text version is to ensure that skimming of tags can reap no reward. An authentication decision (passed or denied) is determined by this comparison.

Step 11: This authentication decision can then either be sent to a border security office manning the checkpoint at which point the officer may wish to conduct a visual check also. Conversely, this system can be used on an unmanned checkpoint and the decision will either allow the traveller to continue their journey, or prevent them from continuing any further.

7.2 Questioning the “key” to the ePassport system

Currently ePassports use 3DES encryption for the data on the RFID tags. Whilst this is an industry standard technology, the issue lies in the allocation of the key to decrypt the data. When designing the current ePassport, ICAO decided that the key to decrypt the data was to be composed using a concatenation of the passport number, holders date of birth, and passport expiry date (in that particular order). If an unscrupulous user was able to copy the passport data as detailed in the meta-analysis above, and could combine this with a high level phishing attack, the

key space could be reduced considerably as detailed by (Sterling, 2006). To alleviate this issue the proposed solution uses message digests. A *message digest* can never be reversed to show the original data hence nobody can ever steal your information from your passport in stealth. The issue with message digests is that because they are never reversed to their original form, somebody could make an ePassport to just hold your message digest and nobody would be any the wiser. Whilst this is theoretically possible, it is not very practical. In order to succeed in this form of attack, the attacker would:

1. have to know the unique password for the ePassport he/she was trying to copy; and
2. have to have the same fingerprint as the legitimate user; and
3. have to look exactly like the legitimate user.

7.3 Layers of security provided by the proposed system

There are 4 layers of security offered by the proposed system.

Layer 1: The data that defines a unique user is used as a query in the passport holders database. If a match is not found it obviously shows that the passport does not exist and hence the owner is attempting to act fraudulently. If a match is found, it verifies that the user does actually exist and the document presented is legitimate.

Layer 2: To ensure that the person claiming to own the details in the passport actually does, a biometric test is used. The user's fingerprint ('searchprint') is taken and compared to the 'fileprint' which belongs to the passport. If a match occurs, it proves that the passport does belong to the bona-fide user.

Layer 3: Now that it has been established that the correct user is the holder of the right passport, it is necessary to ensure that the right chip is in the passport. This step prevents a person from cloning a passport and installing a fake RFID tag in it instead. A unique password which corresponds to the passport in question is sent to the tag. Upon receiving the correct password the chip will respond with data, however if an incorrect password is encountered, the tag will remain dormant and ignore all requests. To ensure someone has not altered the tag to respond at any time, a sequence of passwords can be sent to the tag, all incorrect but one. If the tag responds to an incorrect password, it can be assumed that the tag has been tampered with.

Layer 4: The tag in the passport only stores hashed user values which are created via a one way function and hence can never be reverted back to their original form. This security feature preserves user data as personal information can never be skimmed off the tag even if the right password is found. This means that smart bombs cannot be made to be denominational as the hash string will not reveal information regarding the country of origin etc.

7.4 Confidentiality

Preservation 1: The proposed system's kill tag approach prevents a rogue reader

from tracking users as it is assumed that a rogue reader will not have the tags unique password. Assuming this, a rogue reader will never get any form of response from a tag. Hence the tag owner can travel at ease as their identity is never disclosed.

Preservation 2: In the event that a rogue reader does determine the tags unique password, the information retrieved is in actual fact useless. The tag only stores hashed information which according to the design and manifest behind hashing, can never be processed back into its original form. Hence if a breach occurs and a rogue reader does steal tag data, they have not stolen anything of worth.

7.5 Integrity

The integrity of this system lies in the comparison processes of stored information to retrieved information. The system uses a multi-tiered authentication verification process, by which a user makes an authentication claim (i.e. delivers a passport to the machine) and must then verify that they actually own the passport (via a fingerprint scan). This is again demonstrated when the tag must prove that it belongs to the right passport which belongs to the bona-fide user by communicating with the machine, if, and only if the correct password is received. This phenomenon culminates in a final authentication and verification process by which the tag's hash string is compared to the on file hash string. This multi-tiered process aims at ensuring that changes to data cannot occur, but ultimately if they do occur, one of the tiers of authentication and verification will determine the fraudulence.

7.6 Availability

The user verification system for the tag is a simple means to provide the availability characteristic as this scheme requires a password to read the tag. It is assumed that only a bona-fide user will have the password and hence only makes the tag available to intended users.

7.7 Databases

The user verification system for the tag is a simple means to provide the availability characteristic as this scheme requires a password to read the tag. It is assumed that only a bona-fide user will have the password and therefore the tag is made available to intended users alone.

The reason the two databases (figure 3) are set up into an array is a performance consideration and is intended to reduce the search space and hence allow for practical searching. Using Australia as an example, the top 20 surnames are tabulated and the total frequency of each of the first letters is recorded in figure 4.

The 'W' category holds 160,303 occurrences and when put into perspective accounts for 20.9% of the top 20 occurrences. Applying this figure to the Australian population as a total (approximately 20 million) to provide a rough generalization, it is possible to see that the W database may hold approximately 4 million entries. Considering that 'Google' can search its indexes and return 2,370,000,000 entries

for the letter 'e' in 0.09 seconds it is hence assumed that the intended database model will function efficiently. Data was tabulated using Wikipedia (2007) who gathered their results from IP Australia, Government of Australia.

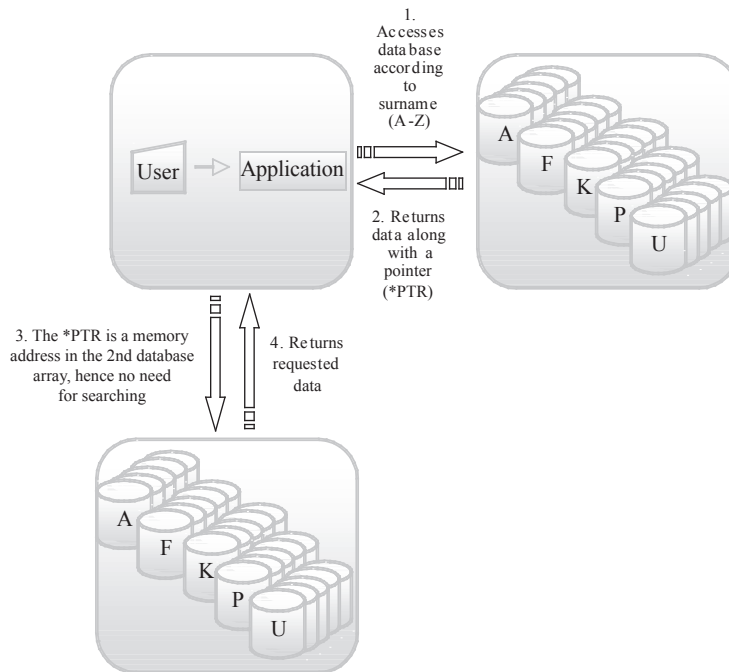


Figure 3- Accessing records from the database

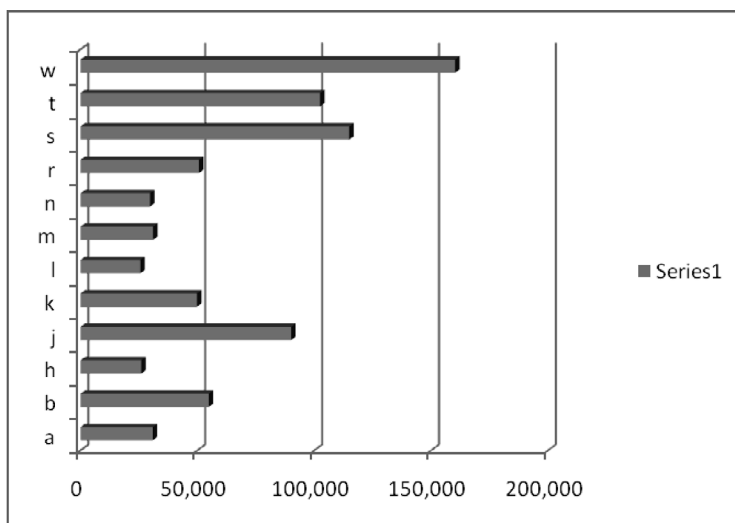


Figure 4- Letter-specific databases for faster searching on surname

7.8 Policy

Currently border security will accept an ePassport with a faulty RFID chip as a legitimate identification document (table 3). This policy is a critical mistake as it circumvents the reason the ePassport was created. If an unscrupulous person disables an RFID chip, the ePassport is now only as secure as a passport without an RFID chip. This is obviously a problem or else why would the government have wished to introduce an ePassport? To remedy this, the policy surrounding the proposed implementation of an ePassport will define a passport with a faulty RFID tag as an illegitimate identification document and will take note of the owner for further investigation.

Table 3- ePassport comparisons

Possible security breach	Current ePassport	Proposed ePassport
Tracking	Breach	Resisted Breach
Killing	Breach	Resisted Breach
Injection attack	Breach	Breach
Blocking security device	Breach	Resisted Breach
Wave injection attack	Breach	Breach
Steal information	Breach	Resisted Breach
Flooding	Resisted Breach	Resisted Breach
TOTAL	Breach=6, Resisted Breach=1	Breach=2, Resisted Breach=5

Tracking: The proposed ePassport can only be tracked if the right password is issued to the tag or else no response will be obtained, however the current ePassport will respond to anything.

Killing: Both implementations are susceptible to a tag being destroyed however the policy for the proposed implementation ensures that this occurrence does not lead to a breach.

Injection attack: Both systems are perceptible to an injection attack if their back-end systems are not configured correctly.

Blocking security device: The Faraday cage that houses the current ePassport fails if the passport is only slightly open (this may occur if thrown into a bag). The proposed enclosure stops the ePassport from opening, hence preventing an inadvertent read window.

Wave injection attack: Both systems are perceptible to this attack as it attacks the core technology.

Steal information: The current ePassport contains encrypted information which can be decrypted, the proposed implementation keeps one way message digests of the data which can never be changed back into the information's original form.

Flooding: Both the new and the proposed system would require so many tags

to actually produce a flooding attack that they could not all be concealed.

8 The irony of it all

“[A]ny system is only as secure as its weakest point of entry” (Microsoft, n.d.).

Whilst this quote was not originally used in the context of ePassports, it applies itself with the same meaning. By reviewing the process of obtaining a passport in Australia the weakest points are quickly identified which render all attempts to secure a passport useless. Figure 5 shows the relationship between these important personal documents. It also shows that the single point of failure is the birth certificate. Zill (n.d.) also takes this point of view and denotes a *birth certificate* is “a “weak” document because it is relatively easy to forge and has no photo or fingerprint requirement (Zill, n.d.). Following the schema presented, once a birth certificate is obtained, a Medicare card can also be obtained. A driver’s license is the next obvious progression as both a Medicare card and birth certificate are in possession. Finally, a passport can be obtained as all the vital government documents are in possession. The previous chronological investigation shows that a passport is not made secure by enhancing the technologies and policies surrounding it, as an illegitimate passport can easily be obtained using fake seminal documents. It is important however to realize that the basis of this paper is not to solve the existence of fraudulent passports, but to ensure that if this particular RFID technology ‘must’ be used, that the technology is applied in such a way that it does not cause new afflictions upon society.

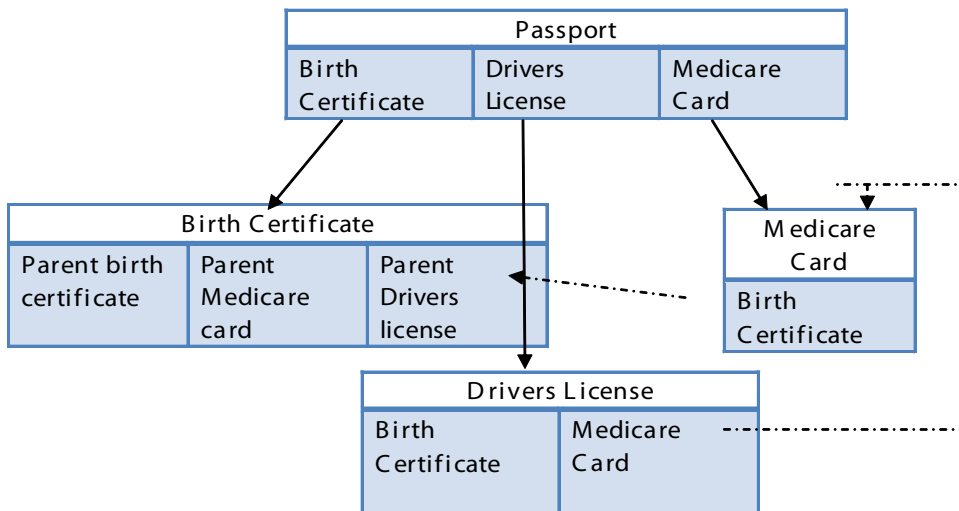


Figure 5- Important personal identification documents

References

- Abzug, M, T. 1991. MD5 Homepage (unofficial). Abzug, M, T. [Online] 1991. [Accessed: 13 April, 2007] <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>.
- Answers.com. n.d. Replay attack. Answers. [Online] Computer Language Company Inc., n.d. [Accessed: 14 April 2007] <http://www.answers.com/topic/man-in-the-middle-attack>.
- Australia, Commonwealth of. 2007. Mobile Telephones Scientific Background. Australian Radiation Protection and Nuclear Safety Agency. [Online] 2007. [Accessed: 30 August 2007] <http://www.arpsa.gov.au/mobilephones/mobiles1.cfm>.
- Bishop, M. 2002. Computer Security: Art and Science. s.l.: Addison Wesley Professional, 2002.
- Brainard, J. Jules A. 2004. Soft Blocking: Flexible Blocker Tags on the Cheap. Washington: Communications of the ACM, 2004.
- Buehrer, G, T. Weide, B, W. Sivilotti, P, A, G. 2005. Using Parse Tree Validation to Prevent SQL Injection Attacks. Columbus: ACM, 2005.
- Centre, Radiation Emergency Assistance. n.d. Definitions related to radiation. Radiation Emergency Assistance Centre/Training Site. [Online] n.d. [Accessed: 4 November 2007] <http://orise.orau.gov/reacts/guide/definitions.htm>.
- Chuvakin, A. Peikari, C. 2004. Protect Yourself Against Kerberos Attacks. WindowsDevCenter. [Online] O'Reilly, 2004. [Accessed: 14 April 2007] http://www.windowsdevcenter.com/pub/a/windows/excerpt/swarrior_ch14/index1.html.
- Department, U.S. State. 2005. U.S. passports get tagged. s.l.: Expanded academic ASAP, 2005.
- Coffee, P. 2006. Passport to a Void Promise; Solving the wrong problem in the wrong way is a stupid tech trick. eWeek. Aug 2006, Vol. 23, 34, p. 16.
- Flexills. 2006. RFID Passport Shield Failure Demo. YouTube. [Online] Flexills, 2006. [Accessed: 15 April 2007] <http://www.youtube.com/wath?v=-XXaqraF7pl>.
- Gonsalves, C. 2005. A Ticket to Trouble; RFID-enabled passports pose privacy, security risks. eWeek. 2005, Vol. 22, 19, p. 33.
- Jules, A. Riverst, L, R. Szydlo, M. 2003. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. Washington: Communications of the ACM, 2003.
- Jules, A. 2005a. RFID Privacy: A technical primer for the non-technical reader. MA: RSA Laboratories, 2005a.
- Kaliski, B. 2005. ravel Security and Function Creep: Thinking about the ePassports in the Long Term. Speaking of security. [Online] 2005. [Accessed: 15 April 2007] <http://www.rsa.com/blog/entry.asp?id=1019>.

- Karjoth, G. Moskowitz, A. P. 2005. Disabling RFID Tags with Visible Confirmation: Clipped tags are silenced. Workshop on Privacy in the Electronic Society. November 7, 2005.
- Khanna, R. 2004. Systems Engineering for Large-Scale Fingerprint Systems. [book auth.] N. Bolle, R. Ratha. Automatic Fingerprint Recognition Systems. New York: Springer-Verlag, 2004.
- Labratories, RSA. n.d. FAQ on RFID and RFID privacy. RSA Labratories. [Online] n.d. [Accessed: 15 April 2007] <http://www.rsa.com/rsalabs/node.asp?id=2120#13>.
- Lamb, G, M. 2006. New 'e-passports' raise security issues; Despite official assurances, some worry that thieves might read chip- toting US passports. Boston: s.n., 2006, p. 13.
- Launch of ePassport press conference. Downer, A. 2005. Canberra: http://www.foreignminister.gov.au/transcripts/2005/051025_ePassport.html, 2005.
- Lettice, J. 2007. How to clone a biometric passport while it's still in the bag. The Register. [Online] The register, 3 2007. [Accessed: 8 August 2007] www.theregister.com/2007/03/06/daily_mail_passport_clone/.
- Microsoft. n.d. Microsoft's approach to secure government systems. Microsoft Government. [Online] Microsoft, n.d. [Accessed: 1 October 2007] <http://www.microsoft.com/industry/government/securityprivacy.mspx>.
- Molnar, D. Soppera, A. Wagner, D. 2005. Privacy for RFID through Trusted computing. Workshop on Privacy in the Electronic Society. November 7, 2005.
- Moses, A. 2006. Passport hacker warns of identity risk. Sydney Morning Herald. [Online] 2006. [Accessed: 14 April 2007] <http://www.smh.com.au/news/security/passport-hacker-warns-of-identity-risk/2006/12/12/1165685661999.html>.
- Munro, K. 2007. SECURITY MATTERS: Broadcast your details with an RFID. February 28, 2007, p. 1.
- Newitz, A. 2006. The RFID Hacking Underground. Wired. May 2006, 14.05.
- Orso, William G.J. Halfond and Alessandro. 2005. AMNESIA: Analysis and Monitoring for NEutralizing SQLInjection. California: ACM, 2005.
- Schoen, S. n.d. Trusted Computing: Promise and Risk. Electronic Frontier Foundation. [Online] n.d. [Accessed: 13 April 2007] http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php.
- Staake, T. Thiesse, F. Fleisch, E. 2005. Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting. Symposium on Applied Computing. March 13-17, 2005.
- Sterling, B. 2006. Arphid Watch: Find Own Foot, Aim Hastily, Pull Trigger. WIRED. [Online] WIRED, 17 11 2006. [Accessed: 8 August 2007] http://blog.wired.com/sterling/2006/11/arphid_watch_fi.html.
- Thorsteinson, P, G. Ganesh, G, A. 2003. .NET Security and Cryptography. Upper

- Saddle River: Prentice Hall, 2003.
- Trade, Department of Foreign Affairs and n.d. The Australian ePassport. Australian Government: Department of foreign affairs and trade. [Online] n.d. [Accessed: 20 April 2007] <http://www.dfat.gov.au/dept/passports/>.
- Wamba, S, F. Lefebvre, L, A. Lefebvre, E. 2006. Enabling Intelligent B-to-B eCommerce Supply Chain. ICEC'06. 2006.
- Want, R. 2004. Enabling Ubiquitous Sensing with RFID. Computer. 2004, Vol. 37, 4.
- Westhues, J. 2003. Proximity Cards. cq.cx. [Online] October 2003. [Accessed: 29 March 2007] <http://cq.cx/prox.pl>.
- Wikipedia. 2007. List of most common surnames. Wikipedia. [Online] Wikipedia, 05 2007. [Accessed: 1 October 2007] http://en.wikipedia.org/wiki/List_of_most_common_surnames#Australia.
- Zill, O. n.d. Crossing borders: How terrorists use fake passports, visas and other identity documents. PBS. [Online] PBS, n.d. [Accessed: 1 October 2007] <http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html>.

19

Improving information security management: an Australian universities case study

Tim Lane¹ and Lauren May²

¹ Graduate, ² Senior Lecturer, Information Security Institute, Queensland University of Technology

Abstract

Universities have an important role to play in the nation's security - as well as the broad social responsibility, the management of information security in Australian universities is increasingly recognized as being strategically important to overall business continuity. Despite this acknowledgement, many issues continue to hamper the effectiveness of real-world information security management in contemporary organisations such as universities. Universities rely heavily on secure IT systems for the support of administration, teaching, learning and research. On one hand data needs to be protected yet remain easily accessible. The practices associated with collecting, storing and using data related to individuals introduces issues of information aggregation akin to dataveillance. One perspective is to acknowledge the inevitability of technologies used in this way and to pursue information security policies and controls that reflect effective strategies accepted by the University community. In order for this to occur an approach is required that takes into account specific organisational requirements in a coordinated and structured manner. This paper proposes a workable security practitioner's management model designed specifically for the enhancement of information security management by operational security staff in Australian universities. The model is based on the results of a comprehensive survey of all Australian Vice Chancellor Council (AVCC) listed Australian universities, with a 100% participation rate. This is significant research as it is the first investigation of its kind in the Australian university sector and has substantive implications for future directions.

Keywords: information security, information security management, security and privacy

1 Introduction

Universities have a role to play in the nation's security. The social implications of this role recognise that universities need to protect both their own information (as individual institutions and as a sector) and as such become custodians for important information and infrastructure in broader society. Looked at from a social perspective, universities host a large number of diverse systems from both a business and academic viewpoint. The sector also characterises a fertile breeding ground for IT exploration and research as well as reflecting and promoting good community standards through their practices, customs and processes. These factors inevitably link universities to playing a key role in the broad security of the nation, albeit not directly Critical Infrastructure Protection (CIP).

It is of interest that research on information security management in the Australian university sector has had very little academic focus. The general research that does exist on information security management often focuses predominantly on context specific models for management or

specific behavioural aspects of managing security – not both. Existing management models tend to concentrate on specific approaches for aspects of security (for example risk management), whereas behavioural aspects often focus on areas such as policy and awareness. What is lacking in the literature is a systemic approach to the management of security specifically in Australian universities. A model which integrates and shows the relationship between the organisational context, behavioural aspects and a functional management model is therefore of practical use to security practitioners.

1.1 The university environment

Universities are amongst the growing number of institutions that increasingly acknowledge the importance of protecting information which is relied upon for business purposes. Despite an acknowledgement of the importance of information security to Australian universities, existing approaches, standards and guidelines for security are not necessarily integrated. They do not provide a single point of understanding for how the process of information security should be managed. There is certainly no overall governance for how information security should be managed within the higher education sector or sector specific recommendations.

The function of information security management in universities tends to be wedged between conformity to corporate mandates linked to the business of providing education on one side, and conversely the open cultural and pedagogical pursuit of academic teaching, learning and research on the other side. Security becomes somewhat of an art form in this environment, requiring navigation through the various complexities of university culture and challenges. One aspect that differentiates universities from a corporate environment is the fact that developers of software and technology in universities attempt to enhance their reputation within

the scientific community, as opposed to basing motivation on purely economic gain. This means that developments tend to occur with a regard for matters that are deemed important to peers, and occur with a level of autonomy from economic driven activity (Kesan and Shah, 2004b). Although this can be beneficial, one key responsibility for universities in this rather exploratory environment is to ensure that abuse of power in information collection, access and dissemination is regulated through reasonable accountability and transparency.

Managing information security in the Australian university environment is complex and remains a challenging area. It tends to be obfuscated by university culture and operating environments. The practical implementation of information security operations therefore requires a solid foundation from which to operate. In determining how information security management could be improved in Australian universities, analysis of the factors and issues that facilitate or impede information security in Australian universities is necessary.

1.2 Literature overview

The literature review involved a broad-brushed approach to ensure adequate coverage of information security. The areas focused on included senior management involvement for effective corporate governance, approaches to operational security management, policy frameworks and content, awareness of security and finally cultural compliance to security. The literature review highlighted that, although the need for information security is acknowledged and considered important, in many cases security is not prioritised in line with its accepted importance. This is reflected by a lack of prioritization, inadequate funding and a general lack of awareness and understanding. These contributing factors include the intangibility of information security issues, inadequate security governance, reactive approaches to managing security and resistance by users due to work practice impacts.

To place historical context on the management of security, Von Solms (2000) provides a perspective through three distinct generational waves. Von Solms proposes that the first generation, the *first wave*, which he calls the *technical wave*, existed up to the early eighties and was distinguished by a very technical approach to information security (such as mainframe terminals and batch Electronic Data Processing (EDP)). During this stage however, the technical administrators realised they would need to obtain further management involvement, giving way to the second wave. The *second wave*, which ranged from the early eighties to the mid nineties, is labelled the *management wave*. This wave is characterised by an increasing interest and involvement by management in information security. This wave supplemented the technical wave and increased the importance of information security.

While improvements were seen under the management wave, the need for a more comprehensive approach was identified – specifically, understanding security risks and the commensurate value and effectiveness of information security to the organisation. This necessitated the ability to measure and compare information security against

a baseline, as well as against other institutions. This saw the development of the *third wave*, called the *institutional wave*. This is the existing wave today. This third wave is represented by the recognition of and interest in, international standards, codes of practice, security certification, cultivating a corporate security culture, and dynamic and continuous security measurement. This third wave also incorporates the ubiquitous requirement for security to transcend traditional notions of purely *restricting* access to data. Restricted access must increasingly co-exist with open access. This dichotomy of open access is not without criticism, as achieving a balance in access and privacy is a subjective process depending on the perspective of the observer. The literature review offered insights and potential explanation for security problems, however further articulation and expansion through specific data gathering was necessary to improve information security management at Australian universities.

1.3 Methodology

The research problem is presented in three questions:

- What is the current status of information security management?
- What are the key issues surrounding information security management?
- How could information security management be improved?

The research project applied a qualitative approach and used two main methods to gather data. The primary data generation method involved applying a survey instrument containing 35 open and closed questions to every Australian Vice Chancellor (AVC) University in Australia. The objective of the survey tool was to identify factors that affect the management of information security in contemporary Australian universities from an operational perspective. The survey participants, therefore, were university professional staff whose responsibilities include the direct management of information security issues. This necessarily limited the scope by not including end-user personnel such as administration staff, academic staff and students.

The participation of all 38 universities represented a 100% survey response rate. The survey was conducted via interviews over the telephone with the IT Director and/or Security Manager equivalents. Each interview averaged 30 minutes and was digitally recorded, then transcribed verbatim to a word processor. This produced over 70 000 words of text, providing a very rich data set for analysis. The secondary data gathering method involved the researcher as an instrument through the role of Information Security Manager at Southern Cross University. This provided opportunity for observation in the field as well as review and analysis of various written material. Qualitative data analysis was applied to data sets in order to identify themes, patterns and relationships. Theoretical constructs were generated from the gathered data, validated from the literature and synthesized into a Security Practitioner's Management Model (see Section 3). The security

model aims to facilitate the transition of expert security practitioner knowledge into implementation. This is achieved through channelling security knowledge through the model's abstracted security framework, focusing on an end goal of cultural compliance towards security.

2 Information security management issues

The findings of the survey were wide ranging for each research question:

What is the current status of information security management? The survey results primarily indicated that the status of information security management in Australian universities varied between each institution dependent on a number of factors. These factors included the security management method, senior management support and involvement, resourcing and funding, the capacity to defend against security threats, the level of IT centralisation, and the overall culture of the organisation. An important finding was that the *champion* of information security (from a strategic and operational management viewpoint) often occupied a non-senior position within the central IT department, reported mainly within the IT department, and yet had wide ranging responsibilities for security impacts across the business. This person often had the most specialised knowledge of security and its impacts yet was not always positioned with appropriate authority for decision making. A critical finding was that a common method adopted to manage information security was cited as being based largely on incident management, reflecting a reactive approach. Comments and views expressed by participants supported the notion that a relatively unstructured and reactive approach to managing security existed in many institutions. This situation was reflected by an ad hoc approach to managing security, a general lack of adoption of standards, a lack of security strategic plans and a cited lack of full integration of security within the business processes and budgets for IT. In summary a broad based enterprise wide approach to coordinated security efforts was not prominent amongst institutions.

What are the key issues surrounding information security management? The key findings identified that a lack of structure in managing information security impacted effectiveness of security efforts across the organisation. The lack of an appropriate structure to integrate throughout the enterprise business processes resulted in security controls applied in an ad hoc manner, ensuing consequences of which easily progress to a reactive nature to be apparent and, eventually, shortcomings in resourcing and funding. A significant gap also existed between desired and actual awareness of information security risks across the university community at large. A major cause for this was cited as the intangibility of security in conjunction with low perception of threat levels. This in turn impacted a broad number of other issues, including work practices, allocation of resources and funding, prioritisation of security, acceptance of the reality of risk, development of clearly written and communicated policy, and general compliance to security.

How could information security management be improved? A structured and

coordinated approach was needed to improve effectiveness of current information security management approaches. Developing a more structured and coordinated management framework for progressing security within the university community was seen as an essential step in delivering improved security management. The human element of information security was seen as one of the greatest barriers to improving security and therefore one of the key factors to focus on for improvement. It is suggested by Kevin Mitnick (2002) that social engineering exploits will increase as technology improves to the point that human weaknesses must be used. Mitnick focuses on the human factor as a weakness that is exploited and cites many examples of how security is generally an illusion. This illusion results from the fact that people from a behavioural perspective wish to view themselves as secure, and tend to believe that others are acting in a manner conducive to overall security, when in fact this may not be the case. The goal of a culture of compliance towards security was commonly highlighted through the research as the best strategic goal to aim for, involving increased awareness of security issues. Engaging senior management to help security resourcing and funding was also seen as a key step. A gap was highlighted in that the use of existing common management frameworks such as AS/NZS 27001:2006 was seen as helpful in what to implement but did not necessarily assist in understanding how to progress security more effectively. An integrated, structured approach was cited as being necessary to improve security management throughout Australian universities. In this context *integrated* relates to bringing together the necessary components and incorporating them into the model itself, while *structured* implies replacing ad hoc approaches with a more clearly defined and coordinated approach.

2.1 Senior management involvement

The coding results established that funding and resourcing is considered to be of significant importance and a major function provided by senior management. This is a function that impacts directly on the capacity to deliver security services. As evidenced through the coding results, participants tended to focus on funding as a primary gauge of support levels by senior management. In broad terms, participants consider senior management support as critical and essential to information security reflected by *Senior Management Support* ranking first out of the top three critical success factors by participants. The survey established clear benefits to those organisations that had in place active reporting and communication structures with senior management. Despite the clear requirement for senior management support for information security, however, less than one third of universities indicated that they regularly reported on information security to senior management.

Key Issues Surrounding Senior Management Involvement: A strong correlation existed between participants who considered senior management to be 'involved and engaged' in security, and corresponding levels of support received from senior management. Similarly, institutions who indicated that support was lacking correlated

with those institutions who reported that senior management was either not 'engaged' with security or had a low level of awareness surrounding security issues. The findings from this survey are also supported by findings from Knapp et al (2006) in their survey involving 220 certified information system security professionals. The results of their study indicate that 'evidence suggests that top management support is a significant predictor of an organisation's security culture and level of policy enforcement'. These findings lead to several primary interpretations. Firstly, senior management support is considered to be critical to the success of the information security function, particularly by way of funding and resourcing. Secondly, notwithstanding other organisational constraints, senior management is more likely to be supportive of security if they are informed and engaged. Thirdly, increasing senior management awareness is most likely to be achieved by ensuring that senior management is included within the overall 'structure' of security management. This is achieved through the process of regular liaison and reporting with the view of increasing understanding and awareness of risk.

Improving Senior Management Involvement: Security is not always considered as being an essential part of corporate governance by senior management, reflected by the lack of established forums or committees regarding security and the fact that security is rarely cited on documentation related to Universities' corporate governance. Fitzgerald (2005) suggests that a security committee has the capacity to facilitate collaboration, ensuring that representative viewpoints are taken into consideration. Without a council or committee, the Information Security officer is effectively working in isolation, attempting to move initiatives forward, and obtaining business management support one person at a time. Similarly, Peltier (2004) maintains that for an information security management program to be effective, an information security steering committee must be established, to act as a champion of security. In order to elevate information security out of the technical realm into the business realm, it is argued that having a structure for security provides a tangible context for senior management (Dutta and McCrohan, 2002). This facilitates senior management viewing security from an enterprise approach and lends support to the security practitioner's management model.

2.2 Security management approach

A clear pattern emerging from the study was the requirement for an improved structure and coordination of how security was being managed. Almost half the participants only *somewhat agreed* that the existing management approach adopted for managing security was effective, and less than one third *agreed* that their approach was effective. This finding has potential for much improvement. This situation clearly indicates that a structured approach is deficient, despite the availability of references such as the *AS/NZS 27001:2006 Information Technology - Security Techniques - Information Security Management Systems - Requirements*, as well as a large range of other security best practices, guidelines, standards and frameworks. The issue is not

so much *what* to implement (although this is extremely important), but more *how* to implement security (that is, the processes and procedures). This problem appears to be commonplace across higher education institutions in Australia, and is reflective of the cultural impediments to security, as well as the emerging maturity of security implementation.

Key Issues Surrounding Security Management Approach: The key issues that emerged with management of security included problems associated with the current management approaches adopted for information security, the lack of coordination of information security impacting effectiveness, conflicting priorities and standards within universities, and the difficulty in easily identifying industry applicable standards. A significant challenge put forward by participants was that existing management standards were not always applicable to universities. Although the 17799 standard (now replaced with 27001:2006) was often quoted as being a preferred management standard, several participants were critical, suggesting that conforming to this standard would be highly time consuming and resource intensive, and that it was not necessarily applicable to the university environment. Another prominent issue arising for many security practitioners was cited as not having control over the IT environment (both technically and culturally) due to IT decentralisation. Conversely, many participants stated that centralisation of IT made life easier in that control over the network could be established more readily. Arguments could be stated for and against centralisation. The main argument for centralisation is improved control over decision making, standards and enforcement of policy. The main argument for decentralisation is based on the increased access to resources outside the main IT department that can, in theory, apply a security focus to their IT environment.

Improving the Security Management Approach: The main three suggestions for improving the security management approach included having a more structured approach, improving awareness and additional resourcing. It was obvious from some comments that a fragmented approach existing in managing security. In part this exists because of a lack of an enterprise security approach, but decentralisation also plays a part. In considering the reactive approach to security incidents and management, it is noted that the perception of risk is often used as the basis for responding. This was an issue that was raised many times, by way of *it won't happen to us* where perception was dominant. Kotulic and Clark (2004) note that threats and vulnerabilities are generally not considered until after a security breach has occurred, a view reinforced by participant comments in the interviews. This highlights and reinforces that the reactive state of managing via security incidents is due to risk management being implemented in accordance with the perception that *it won't happen to us*.

2.3 Security policy

Universities vary widely in approaches to security policy. This is seen in

differences such as some universities having active committees reviewing and signing off on template-based policies with active input from policy developers. Other institutions cited that they simply *need to start* on policy development. In the context of this paper we refer to *processes* and *procedures* as being components of *policy* in the generic sense, without formalising the concept.

A large majority of participants considered policy to be instrumental in establishing a culture of compliance to security, although many acknowledged challenges associated with policy enforcement. Factors contributing to the effectiveness of policy included having an established policy process that included a formal approval mechanism, engagement of key stakeholders, backing from senior management, as well as active communication and awareness of policy. Those participants who felt the policy process was ineffective cited a lack of participation, delays in policy approval, unwieldy policies, a lack of policy review, and difficulties in gaining policy compliance.

Key Issues Surrounding Security Policy: For policy to be effective, several attributes were noted as being required. These include senior management support, appropriateness of policy to the organisation, awareness of policy and its meaning, and available procedures for implementation. Several major themes stem from this area. Development of policy in terms of the actual writing of policy, coverage of policy and how policy should be constructed were raised as issues. The appropriate context for policies, including business requirements down to the low level procedures for policies, appeared to often be *missing links* for final implementation of policy. The security practitioner's model attempts to capture this requirement through its layered approach by ensuring the *Contextual* layer provides business requirements, and that the *Operational* layer includes procedures and operational support. In practice, there is little evidence to suggest that any of the recognised and documented policy development processes are rigorously adopted. Instead, as with other research, anecdotal evidence suggests that areas of risk are considered and policy statements are basically adapted from existing sources (Maynard2002). As noted by Hone and Eloff (2002), difficulties are associated with this process in that they do not truly reflect the culture of the organisation. An end result of this is that they do not result in a document that effectively provides relevant direction for information security in the organisation. This is a key issue as a theme emerging from data analysis indicated that the relevant issues were more associated with engaging people in policy development and gaining compliance to policy, rather than obtaining written policy statements.

Improving Security Policy: One of the main problems with policies is inappropriate abstraction according to Gaskell (2000). This was an issue mentioned in the interviews, where policies were inappropriately written as either high level or very detailed, where the level of abstraction is inappropriate for the audience. It is clear that a differentiation between security policy and supporting security procedures is required in these types of circumstances. This research recommended adopting

the layered policy abstraction and refinement method as proposed by Baskerville and Siponen (2002) and Abrams and Bailey (2001). The abstraction and refinement model effectively looks at 'abstracting' and 'refining' policy at a level where it is most effective and relevant to the end user. The research also detailed the essential elements contained in the international standards to provide approach direction on security policy (Hone and Eloff, 2002).

2.4 Security awareness

The area of security awareness highlighted that awareness raising activities are not well structured. Awareness is raised predominantly by occurrence of incidents rather than a structured, targeted program of activities. The ad hoc approach to raising awareness is reflected by the fact that less than 15% of participants stated they had adopted the preferred formal or structured awareness program. Despite opinions that raising security awareness was an important priority, less than five percent of participants agreed that existing activities resulted in raising security awareness levels adequately. Nearly 50% of participants *somewhat agreed*, and over one third *disagreed* on the adequacy of activities, indicating that awareness raising activities are far below requirements.

Key Issues Surrounding Security Awareness: Although resourcing was cited as the main barrier to increasing awareness, cultural reasons and a lack of prioritisation also impacted raising awareness activities. The types of issues raised included the lack of awareness of the university community, particularly end users, a transient student base, and lack of awareness by Management and Executive. The lack of a skill set for security, and the lack of a coordinated approach to raising security awareness, the resources and time required to raise awareness were also mentioned. The issue appears to be one of a lack of mandate for structured awareness activities. Despite its acknowledged importance, focus and effort on security activities was lacking. Clearly a conflict exists between the importance placed on security awareness and the priority actually given to improvements in this area. Insufficient communication from security sections in universities causes users to construct their own models of reality on possible security threats and the importance of security. This study indicated the model of reality constructed by the user could be wildly inaccurate due to insufficient knowledge. This caused security areas to view users as inherently insecure, and users to view security people as obstructionist in mechanisms deployed, creating a vicious cycle. Understanding people's motivation and deconstructing any false sense of realities towards information security, therefore, is a useful exercise when undertaking awareness activities.

Improving Security Awareness: One of the key issues in security awareness in universities is exacerbated by the fact that universities have a transient student base. There needs to be a strategic, targeted and continuous program in place to increase awareness in universities, one that is adequately funded and resourced. Users will resist change if they cannot see the benefits, or the process is difficult or time

consuming. It is also necessary to balance awareness raising activities with transparent technology based policy enforcement processes that minimise requirements for end user awareness and voluntary compliance. The research adopted recommendations by Siponen (2000) who argues that all information security awareness programmes should use a 'framework and content' approach. The framework aspect would use an appropriate structure and leverage from the use of standards and guidelines, while the content approach focuses on appropriate internalization of guidelines. It is worth considering that the approaches used in information security awareness programmes should satisfy the requirements of behavioural theories in order for end users to understand why they should follow security guidelines.

2.5 Security compliance

The section on compliance covered a diverse range of areas related to security which indicate that higher education institutions could benefit from improved governance over information security. The fact that a lack of measurement presides over security indicates that coming to terms with the management of security is difficult. The lack of measurement indicates that security has attributes of intangibility of risk, and its value to the organisation is not always clearly recognised. A poor *culture of compliance* was cited by participants as the number one barrier to improving overall compliance to security, particularly in a decentralised environment. This was followed by issues with funding and resourcing, and then awareness and understanding.

Factors *critical to the success of information security management* focused on senior management support, strategic governance, and awareness and education. When asked what the critical success factors were for effective security management, participants responded largely with a focus on the engagement and support from senior management, ensuring that the correct structure and governance framework was in place, underpinned by policy (structure and framework included both governance structure and technical architecture), followed by ensuring that awareness and education rates were high so as to facilitate a culture of compliance.

Key Issues Surrounding Security Compliance: The core issue surrounding compliance to security centred on the fact that drivers for regulatory compliance are still emerging for Australian universities. Another issue for compliance is associated with the fact that the tangibility of measuring the effectiveness of security spending is very difficult. Loose compliance drivers, therefore, linked with the difficulty in understanding the effectiveness of approaches has resulted in compliance being fragmented across the organisation.

Although technology is a key factor in protecting systems, the people and processes that are integral to ensuring that technology is appropriately placed were indicated as needing to be coordinated under a successful management framework. This is particularly the case considering that as demand for open systems expands, more threats emerge, more point based technology solutions appear, and

consequently a patchwork of technology based systems develops. Moving forward it will be increasingly vital that universities are able to understand, measure and demonstrate the effectiveness of security approaches, in order to ensure that necessary standards can be met to achieve emerging regulatory compliance.

Improving Security Compliance: Despite security being a recognised issue, many organisations lack a comprehensive understanding of security issues and the required levels of controls to adequately mitigate risks is not always clear. A lack of availability and comprehensiveness of security guidelines and standards is not the issue as these are already available to a large extent. Obtaining compliance to information security standards faces a number of challenges that Nosworthy (2000) describes as ‘balancing factors’ between risk and control. In many cases universities have the belief that because it hasn’t happened to them it never will. This type of mindset results in a reluctance to fully commit to information security.

Obtaining a culture of compliance requires a change at the individual, group and organisational levels (Vroom and Von Solms, 2004). Security must be viewed as a multi-faceted problem which requires a comprehensive solution to encompass physical, procedural and logical forms of protection. The security management model provides the necessary view to facilitate this.

3 Security practitioner’s management model

The authors based the design of this model on the results of the survey, where the basic concept of the management model is an adaptation of the Zachman Architecture Framework (Stephenson, 2005 and Zachman, 1987). Detailed survey outcomes are available from the author’s Masters thesis. The resulting security practitioner’s model (Figure 1) provides a way to conceptualise the fundamental challenges faced by the security practitioner in progressing security implementation within Australian universities. The major challenges can be thought of as requiring a way of understanding not so much what to implement, but how to conceptualise and move forward with implementation in order to progress it within the institution.

3.1 A systemic approach

This model, although generically applicable, is designed specifically for Australian university information security practitioners, whose role encompasses a responsibility for security implementation at the operational level. The model facilitates an improved process for information security management at the operational level by providing a reference for security practitioners to consider how best to transition security knowledge into effective implementation. Relevant, validated and fundamental aspects are incorporated into the practical management model which integrates and clearly shows the relationships between the layered organisational contexts.

At the security practitioner’s level, the major goal of the model is to allow practitioners to apply the management of information security in a structured

and cohesive manner. At the broader organisational level, the major goal of the model is to increase the transparency and effectiveness of the information security process towards facilitating organisational requirements (the business function). This transparency is directly beneficial to the findings in Sections 2.1 and 2.2.

From the security practitioner's perspective, an approach needs to provide a meaningful structure for progressing information security in an environment where competing priorities exist. This approach, underpinned by communication and awareness, should be focused on developing the organisation's culture of compliance. Continuous security improvements applied through the framework can achieve regulation of an aspired culture of compliance. This approach relates directly to Section 2.1 and, consequently, to potential improvements by all in terms of security compliance (Section 2.5) and improved policy approaches (Section 2.3).

The model is premised on findings from the study as well as fundamental assumptions well evidenced in the literature. First, that information security management is most effective when a structured process is aligned across the organisation, from the senior executive down to the daily operational practices of end users. Second, that the use of controls and standards alone is not enough; developing a culture of security is an end goal of the model requiring communication and awareness across all layers of the organisation. Third, that the resultant compliance to security must be continuously monitored and adjusted through the adoption of a review mechanism such as the ISO 27001 *Plan, Do, Check, Act (PDCA)* model (27001:2006), or another similar audit-based monitoring and corrective action process.

3.2 The use of standards in the model

Best practices are recognized as playing an extremely important role in information security management. Standards such as AS/NZS ISO 27001:2006, and Cobit (2000) are accepted and well-regarded globally. Any of these information security management standards can be incorporated into the model, as can any hybrid best practices.

Although a selection of various elements of disparate best practices can be aligned to suit the organisation, the use of best practices needs to be applied in context to organisational needs. If treated purely as a technical guide, information security standards tend to be unfocused and costly. By incorporating the standard into the model, the implementation of these best practices becomes consistent with the business risk management and control framework (IT Governance Institute, 2005).

3.3 Process flow through the model

The model begins by processing knowledge (gained from information security understanding, broader organisational knowledge, information technology expertise, management ability, best practice frameworks, and previous experiences of the

individual practitioner) into the institution's security programme. This knowledge must be channelled into an appropriately designed interface to the organisation in order for security practices to be gradually incorporated into daily processes and procedures. This is necessary as part of developing the culture of the organisation as inappropriate application of security procedures can result in an expensive or unacceptable overhead (May, 2003). The interface ideally should be a structured and well accepted information security management programme.

The information security management programme links into a five-level abstracted layered structure which begins at the business strategic level, represented as the contextual level, and is traceable through the organisation finishing at the operational layer. Across the layered structure, the process of communication and awareness facilitates the end by-product, a culture of compliance. The central goal of the model is the required organisational level of a culture of compliance with the depicted external and internal influences viewed as inter- and intra-organisational factors impacting culture. The resulting compliance levels are then re-processed into the knowledge that feeds back into the framework. A continuous loop is thus established that represents the transition of knowledge towards a culture of compliance.

The Contextual Layer is the business context of the organisation representing the organisation's security posture. The Logical Layer symbolizes the virtual constructs of security. The Physical Layer denotes the actual physical security including infrastructure. The Operational Layer involves people and support mechanisms.

Channelling Security Practitioner Knowledge The findings from this report and other research on information security management support the concept of the security practitioner's role being one of a knowledge gatherer, with the challenge of implementing knowledge. While the above mentioned frameworks provide guidance on how information security should be implemented, it can be helpful to view information security from the practitioner's perspective as a challenge of implementing knowledge.

Interfacing Through an Information Security Management Programme Security practitioners need to transition their information security knowledge into an implementation of security solutions, and should therefore pursue a management model that coordinates an operational, tactical and strategic approach to security. The proposed security practitioner's model adapts and leverages existing enterprise architecture models for security. The result is an enterprise framework that progresses security knowledge into a culture of compliance.

Leveraging Zachman, Sherwood and Stephenson Frameworks The abstracted layers of the model are well grounded and leverage off previous enterprise framework concepts originally conceived by Zachman, which were later extended and applied specifically to security architecture by Sherwood (Vroom, 2004). Zachman initially developed the Zachman framework, a six layer abstraction matrix which was later modified by Sherwood into the SABSA methodology (SABSA being the *Systems*

and Business Security Architecture). This was then later referenced as the *Sherwood Applied Business Security Architecture*. Stephenson (2005) later researched the model and considers the model in a wider context as a 'Security Architecture Reference Model' (SARM) noting its adaptability to security as well as other more generic areas. The primary point of evolution of the model has been away from the SABSA model according to Stephenson (2005), such that the model can be applied effectively to other generic information systems applications.

Establishing Boundaries of Control for Security Domains The research undertaken in this project found that 'resourcing' was consistently cited a major obstacle to improved security management. In many institutions improved levels of resourcing may not be easily achievable, and therefore processes themselves need to be examined. Detert, Schroeder, and Mauriel (2000) advocate reviewing processes through identification of cultural configuration and patterns, and within their eight-dimensional framework reference *orientation and focus* as being related to examining and improving processes. The implication is that where resources are not easily increased, processes must be examined for improvement. Those processes should be considered in terms of business requirements as opposed to simple tactical solutions, and the layered abstraction model facilitates this way of thinking.

3.4 Communication and awareness

The use of communication and awareness in the model is so obviously apparent that reference to it is best placed in relation to its role in influencing behaviour. The role of communication and awareness in the model needs to be directed towards a goal of normalising behaviour, in other words developing a culture of compliance. Existing theory agrees that behaviour is related to the interaction of ability, motivation and working conditions (Siponen2000). Therefore communication towards normalising behaviour should be taken into account in these interactions.

The two main ways of influencing changes in human belief in order to influence behaviour are thought to occur through both active participation and persuasive communication (Siponen,2000). Motivation of people towards information security is important and Siponen (2000) describes motivation as dynamic in nature and only lasting from minutes to weeks. This correlates with shorter activity levels, where attitudes are of a more static internalised nature, and relate mainly to the quality of actions.

Siponen (2000) references a behavioural science framework for improving information security awareness. The framework is based on existing theory, including theory related to intrinsic motivation, planned behaviour and the Technology Acceptance Model (TAM). Siponen (2000) maintains that certain persuasion strategies based on motivational factors are likely to assist listeners to internalise security guidelines. These strategies should be used in addition to the use of a reward and sanction system, which takes into account the aforementioned theories in the

behavioural science framework. Siponen (2000) rationalises that a 'set of persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions' should be used where appropriate.

3.4.1 External and internal influences

The model takes into account factors that are internal and external to the organisation which are likely to impact on the culture of the organisation and therefore influence behaviour. Although most of these factors will be outside the security practitioner's control, it is helpful to be able to conceptualise and categorise the types of influences.

3.5 Organisational culture of compliance

The security practitioner's security management model has an end goal of a culture of compliance where behaviour reflects compliance to information security policy and practices. Information security policies are the guidelines that dictate the rules and regulations of the organisation, which in turn govern the security of information (Vroom2004) and are therefore significant determinants of culture. Organisational culture includes the ideas shared by the people within the organisation and communicated between each other. This system of learned behaviour and culture is cited as the single most important factor accounting for success or failure in an organisation (Vroom and von Solms, 2004). One goal of an organisational culture of compliance, therefore, seeks to ensure that rules and regulations are normalised as learned behaviour. Recognising an organisation's culture of compliance towards information security is a major factor in understanding how to manage information security and is a key determinant of the success of information security.

The PDCA model (27001:2005) is widely referenced in standards as a continuous improvement quality model which can be applied to all processes.

4 Validation

By its very nature, this study has a strong applied research component; consequently the survey adopted a qualitative research model whose methodology involved a broad approach to the study of real-world phenomena. This broad approach is reflected through a pragmatic, inductive and interpretive method based in a natural setting (the university environment) and enhanced through an attempt to capture and define people's experiences, as recommended by Marshall and Rossman (1999). The main analysis technique applied to the survey responses was thematic analysis which involves cross-referencing data for the purpose of identifying emerging themes and patterns. The thematic approach was supported by the triangulation of observations, participation, literature reviews and the survey instrument. This approach tends towards an inductive model for illuminating processes, one recommended by Miles and Huberman (1994) to ensure a visible, easily recognizable and clearly objective methodology. This open structure supports

and validates the research from both the academic and practitioner perspectives.

Universities are inevitably social actors in the development of technology and have origins in the social rules of how individuals participate with technology. As universities come to grips with managing data from a privacy and accessibility perspective, greater attention will need to be paid to developing and adopting an approach that is appropriate for individual institutions. The model has the capacity to provide a systemic approach in relation to security threats, as well as to privacy aspects due to its holistic organisational wide approach. This is an important aspect as there are growing calls for proactively designing security technologies to regulate as an alternative or in conjunction with the law. For example, digital rights management technologies are supplanting the rights established by copyright law on how people can access and use content (Kesan and Shah, 2004b). The security practitioner's model is currently being trialled at Southern Cross University. The model provides a holistic structure which has substantially improved the credibility of the security management program.

Invariably, when faced with the need for privacy and accountability, individuals demand the former for themselves and the latter for everyone else (Brin, 1998). The model plays a role in ensuring that security achieved accountability without extending to invasion of privacy. This decision balances security by meeting essential security requirements related to authentication (thereby providing accountability for use) without violating individual privacy. This leads us to the observation that universities provide an environment that both nurtures and cultivates software development, and software is the law of cyberspace that affects fundamental issues such as privacy, trust and accessibility (Shah and Kesan, 2004). In effect, universities are comprised of a group of actors who are subject to cultural aspects that shape their activities, norms and behaviours, in turn impacting both security and privacy aspects within society.

The proposed security practitioner's management model represents a synthesis of the emergent themes, patterns and theories derived from the survey data subsequent to data analysis. The model provides direction for the practitioner in approaching fundamental challenges that impinge upon the effective management of information security. This is achieved through an enterprise and holistic approach to the issues that require a way of understanding not so much what to implement, but how to think about implementation in order to progress information security within the organisation.

5 Conclusion

Universities participate in the recruitment of audiovisual, communications and computer database information on individuals and research material. As universities are an important foundation of society, the future of who and how this aggregation of information is controlled becomes an increasingly important issue. From a macro perspective, applying a transparent and accountable process to the collection, storage

and use of information is seen as a critical step towards finding a balance between protecting civil liberties and state based control. This cannot be achieved without taking into consideration individual requirements for specific institutions within the wider context of society. Information security management in Australian universities plays an important role in establishing standards and demonstrating effective methods for information security management.

This research improves the current understanding of information security management in Australian universities by synthesising the findings of the study to a theoretical framework (the Security Practitioner's Management Model). Effectiveness of the model is measured most noticeably at both management and staff levels. Management at the university recognise and accept the *knowledge gathering* role of the information security manager's position, and now not only support the role, but expect this role to be involved in security research. General awareness of university staff has increased with a particular emphasis on individuals' willingness to participate in the security management process, as both transparency and comprehensiveness of process are evident.

References

- Abrams, M. & Bailey, D., (2001), Essay 5: Abstraction and Refinement of Layered Security Policy. Information Security: *An Integrated Collection of Essays*. California USA, IEEE Computer Society Press.
- Baskerville, R. and M. Siponen (2002) An Information Security Meta-Policy for Emergent Organisations. *Logistics Information Management* 15(5/6): 337-346.
- Brin, D., (1999), The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom?, Perseus Books Group, New York.
- Detert, J., Schroeder, R. and Mauriel J. (2000), A Framework for Linking Culture and Improvements in Organisations, *Academy of Management Review*, Vol. 25, No. 1, pp. 850-63.
- Dutta, A. and McCrohan, K. (2002) Management's Role in Information Security in a Cyber Economy, *California Management Review*, Vol. 45, No. 1, pp. 67-87
- Fitzgerald, T. (2005), Building Management Commitment through Security Councils. *Information Systems Security*, Vol. 14, 2 pp. 27-36.
- Gaskell, G. (2000) Simplifying the Onerous Task of Writing Security Policies. ISRC, Queensland University of Technology (QUT). *Proceedings from AUUG Inc. Security Symposium, Brisbane Australia*.
- Höne, K. and Eloff, J., (2002), What Makes An Effective Information Security Policy?, *Network Security*. Vol. 6, pp. 14-16.
- IT Governance Institute, (2005). '*Aligning CobiT, ITIL and ISO 17799 for Business Benefit, 2005*'.
- Kesan, J and Shah R. (2004a), Nurturing Software: How Societal Institutions Shape the Development of Software, University of Illinois College of Law, Research Paper No. 04-07, Accessed from Social Science Research Network

- on 30Jul2007.
- Kesan, J and Shah R. (2004b), The Recursive Regulatory Model, Journal Article downloaded from Goveringwithcode.Org, accessed 30July2007.
- Knapp, K., Marshall, T., Rainer, R. and Ford, F. (2006) Information Security: Management's Effect on Culture and Policy, *Information Management and Computer Security*, Vol. 14, No.1, 2006, pp. 24-36.
- Kotulic, A. and Clark, J., (2004), Why There Aren't More Information Security Research Studies, *Information and Management*, No. 41, pp. 597-607.
- Marshall, C. and Rossman, G. (1999) *Designing Qualitative Research*, Sage Publications, London.
- May, C., (2003), Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy, *Computer Fraud and Security*, Issues 5, pp. 10-13.
- Maynard, S. and Ruighaver, A. (2002) Evaluating IS Security Policy Development. Presented at *3rd Australian Information Warfare and Security Conference 2002*.
- Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis*, Sage Publications.
- Mitnick, K., Simon, W. (2002) *The Art of Deception: Controlling the Human Element of Security*. Chapter 1 Security's Weakness Link and Chapter 16 Recommended Corporate Information Security Policies. Indianapolis, Indiana, Wiley Publishing Inc.
- Nosworthy, J. (2000) Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? *Computers and Security*. Vol 19, pp. 337-347.
- Peltier, T. (2004), Developing an Enterprise Policy Structure, *Information Systems Security*, Vol, 13, No. 1, pp.44-50.
- Sherwood, J., Clark, A. and Lynas, D., (2003) *Systems and Business Security Architecture*, White Paper sourced from the Internet 13th July 2006 at: <http://www.sabsa-institute.org/whitepaperrequest.aspx?pub=Enterprise+Security+Architecture>
- Stephenson, P., (2005), S-TRAIS: A Method for Security Requirements Engineering Using a Standards Based Network Security Reference Model. Conference *Proceedings from SREIS 2005*, Accessed from the Internet 14th July 2006. <http://www.sreis.org/old/2001/papers/sreis018.pdf>
- Von Solms, B. (2000) Information Security – The Third Wave? *Computers and Security*. Vol. 19, No. 7, (2000) pp. 615-620.
- Vroom C. and Von Solms, R. (2004). 'Towards Information Security Behavioural Compliance', *Computers and Security* (2004) 23, pp.191-198.
- Zachman, J. (1987) A Framework for Information Systems Architecture, *IBM Systems Journal*, Vol. 26, No. 3, 1987.

Author Biographies

Ms Roba Abbas has recently graduated with first class honours in Information and Communication Technology (majoring in Business Information Systems) from the University of Wollongong. She is currently the product manager at local web software development company Internetrix, and is involved in the areas of product 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 presented at last year's RNSA Social Implications workshop and her honours thesis is available at <http://ro.uow.edu.au/thesesinfo/2/> • roba06@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

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

Mr Muhammad Usman Iqbal is a PhD candidate in the School of Surveying and Spatial Information Systems, Faculty of Engineering, The University of New South Wales (UNSW), Australia. He holds a Masters degree in Computer Science from UNSW and a Bachelors degree in Computer Science from the University

of Karachi, Pakistan. His area of research is Privacy-aware Automotive Telematics where he seeks an understanding of 'locational privacy' and the importance of designing privacy-respecting technology solutions. Usman's work is supported by the 'Metadata Scholarship' from OMNILINK Pty. Ltd., where he has also developed a GIS Metadata Software Portal. Prior to post-graduate studies, Usman has worked in industry as a Software Engineer for 2 years. He is a student member of IEEE, ACM, Australian Privacy Foundation (APF) and the Australian Computer Society (ACS). m.iqbal@student.unsw.edu.au

Mr Tim Lane has recently been awarded his Masters by Research (IT) at the Queensland University of Technology. His thesis focused on information security management in Australian Universities. Prior to this Tim has completed a Bachelor of Management and Professional Studies (2002) through Southern Cross University, and an Associate Diploma of Information Technology at Gold Coast Institute of TAFE. Tim currently is the Information Security Manager at Southern Cross University, responsible for the development and maintenance of an organisational wide information security management programme. Tim's interest in information security extends across management, behavioural and technology aspects. tlane@scu.edu.au

Dr Samsung Lim is a Senior Lecturer in the School of Surveying and Spatial Information Systems, The University of New South Wales (UNSW), Sydney, Australia. For the past fifteen years his research has been focused on the area of GNSS and GIS. Samsung's research interests are in theoretical problems related to RTK-GPS and applying geo-spatial information technologies to real-world problems. In 2005, Samsung developed an address-based search tool in conjunction with contemporary web-map services such as Google Earth. Samsung received his B.A. and M.A. in Mathematics from Seoul National University and his Ph.D. in Aerospace Engineering and Engineering Mechanics from the University of Texas at Austin. s.lim@unsw.edu.au

Associate Professor Doug MacKinnon is the Director of the Centre for Transnational Crime Prevention, Faculty of Law, at the University of Wollongong. The CTCPP was established in 2000 and officially opened in June of 2001. CTCPP focuses on the operation, prevention and responses to organised criminal activities that impact on regional and global security. Doug was previously with the Australian Federal Police in New South Wales, Australia. His research interests are in transnational dimensions of maritime crime. dougmack@uow.edu.au

Professor Brian Martin is Professor of Social Sciences in the School of Social Sciences, Media and Communication at the University of Wollongong, NSW, Australia. He is the author of 12 books and hundreds of articles on nonviolence,

dissent, democracy, information issues, scientific controversies and strategies for social movements. bmartin@uow.edu.au

Dr Lauren May was awarded a PhD, MASc (Research) and BASc (Maths) in 2002, 1996 and 1990 from Queensland University of Technology. Her research degrees are in cryptology. Lauren worked full-time for the Information Security Research Centre (now Information Security Institute) at QUT in a research assistant position from 1991 to 1997. She commenced working as an academic in the School of Software Engineering and Data Communications in 1997, firstly as a Lecturer then a Senior Lecturer in 2002. Lauren currently holds this position and continues with her research through the Information Security Institute. In recent years she has developed interests in cross-disciplinary research areas building upon her solid research foundations in information security. l.may@qut.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 40 refereed papers and is currently working towards the completion of her second book. 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 was invited to deliver 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

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 Universités Etrangères' appointment at the Université D'Orléans (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 Nicholas 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 Marcus O'Donnell is an Associate Lecturer in the School of Journalism and Creative Writing, University of Wollongong where he has played a key role in the establishment of the new Bachelor of Journalism. Prior to this he worked widely as a journalist and editor. He is currently completing his PhD on "Apocalyptic Narratives in News and Popular Culture" in the Faculty of Humanities and Social Sciences at the University of Technology Sydney. His research interests centre around a narrative model of news media and popular culture and he has presented at a number of interdisciplinary conferences and published in a number of journals looking at the intersection of law, media, religion, terrorism and popular culture. marcuso@uow.edu.au

Dr Lucy Resnyansky Research Scientist, Command & Control Division, Defence Science and Technology Organisation (DSTO) has graduate degree in Linguistics (1985) and PhD in Social Philosophy (1994) from Novosibirsk State University (Russia); and PhD in Education (2005) from the University of South Australia. She has been affiliated with the University of Wollongong, Macquarie University, and the University of Western Sydney. Her research experience covers sociological studies of attitudes, beliefs and motivation; theoretical modelling and empirical studies of human communication; analysis of media and advertising; and ethnographic studies of work practices and human performance. Her research interests are in such areas as social semiotics, sociology of science, social informatics, and sociocultural theories of cognitive action, learning and meaning. 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. mrrix@uow.edu.au

Associate Professor Gregory Rose is an international law specialist with substantial practical experience, including as Head of the Trade, Environment and Nuclear Law Unit in the Legal Office of the Australian Department of Foreign Affairs and Trade. Gregory's expertise has enabled him to train officers of the Royal Australian Navy in legal aspects of maritime security, to deliver counter-terrorism law training courses to officials in South East Asia and to be an adviser to the Australian Minister for the Environment. His research interests concern international law standards and their implementation in the fields of counter-terrorism and marine environment. grose@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

Mr Matthew Sirotych, Honours Candidate, School of Information Systems and Technology, Faculty of Informatics, University of Wollongong. Matthew's research interests are predominantly in the area of security and radio-frequency identification. msirotych@gmail.com

Ms Holly Tootell is a Lecturer in the School of Information Systems and Technology, Faculty of Informatics at the University of Wollongong where she teaches subjects in the areas of social implications of information technology and innovation. Holly's research interests are the social and privacy implications of technology, with a focus on issues relating to national security. Her PhD used media content analysis to establish an understanding of the interplay between privacy, liberty and security when applied to location-based technologies. Holly is the Secretary of the Australian chapter of the IEEE Society on Social Implications of Technology

(SSIT). holly@uow.edu.au

Dr 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