The First Workshop on the Social Implications of National Security

The Social Implications of Information Security Measures on Citizens and Business

29 May 2006
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:	Dr Chris Flaherty, University of Melbourne
Node Leader:	Prof Joseph Lai, UNSW@ADFA
Node Leader:	Prof Ed Dawson, Queensland University of Technology
Outreach Manager:	Athol Yates

Editors: Michael, K. & Michael, M.G.
Publication Title: The First Workshop on the Social Implications of National Security (Workshop on the Social Implications of Information Security Measures on Citizens and Business, 2006)
Series: Research Network for a Secure Australia (RNSA)
Publisher: University of Wollongong, Centre for eBusiness Application Research (CeBAR) (School of Information Technology and Computer Science)
Contact Details: Tel 02 4221 3937, Fax 02 4221 4170, University of Wollongong NSW 2522
Conference Websites:
http://www.secureaustralia.org/ & http://www.uow.edu.au/~katina/workshop.pdf
Publication Year: 2006
Format: Book (hardcopy $45 AUD; softcopy $30 AUD from http://www.homelandsecurity.org.au/publications.html)
Cover and text layout: Anthony Petre
ISBN-13: 978-1-74128-118-7
ISBN-10: 1-74128-118-0

Foreword

The 2006 Workshop on the *Social Implications of Information Security Measures on Citizens and Business* 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 2006, the workshop was held on the 29th May, at the Function Centre at the University of Wollongong between 8.30 am and 5.00 pm.

The Workshop was organised by RNSA members of the Centre for eBusiness Applications Research at 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 Security v Civil Liberties.

Workshop participants will learn about the current and potential status of information security measures in Australia, consider their implications on citizens and business, and identify their impact on legislation and privacy at a local and global level.

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

The workshop included papers by Professor of Management Mary Barrett, Professor of Law Simon Bronitt (invited keynote), Professor of Software Engineering Peter Croll, Professor of Computer Law Margaret Jackson, Professor Sociology of Communications Supriya Singh, and Professor of Transport Systems Marcus Wigan (invited keynote). Other professionals included Roger Clarke Principal of Xamax Consultancy, DSTO research scientist Dr Lucy Resnyansky and the Information Security Institute's Dr Lauren May.

The Workshop Proceedings contains only peer reviewed papers. The acceptance rate was 38%. 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 made extensive comments to at least two revisions of 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 their dedication to researching and writing up the results of their individual projects.

Program Committee

With respect to the organisation of the *Social Implications of Information Security Measures* workshop, the Chairs received feedback from the following RNSA members.

Professor Lyn Batten
Professor Ed Dawson
Dr Christopher Flaherty
Mr Anant Gupta
Associate Professor Priyan Mendis
Professor Rei Safavi-Naini
Professor Jennifer Sebbery
Mr Athol Yates

We would also like to acknowledge the support of Professor Philip Ogunbona, the Head of the School of Information Technology and Computer Science (SITACS) at the University of Wollongong.

Workshop Committee

Chair: Dr Katina Michael
Co-chair: Holly Tootell
Co-editor: Dr MG Michael
Centre for eBusiness Applications Research (CeBAR), University of Wollongong

Reviewers

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

Associate Professor Carole Alcock
Professor Joan Cooper

Associate Professor Sandy Gordon
Associate Professor Peter Hyland
Adjunct Professor Adrian McCullagh
Dr Katina Michael
Dr MG Michael
Ms Holly Tootell

Table of Contents

1

The proliferation of identification techniques for citizens throughout the ages

Katina Michael and MG Michael

School of Information Technology and Computer Science, University of Wollongong

Abstract

Manual identification techniques date back to ancient times, however the need to identify individuals has heightened particularly since the Industrial Revolution. This paper traces the use of identification techniques throughout the ages and focuses on the growing importance of citizen identification (ID) by governments. The paper uses a historical approach beginning with manual techniques such as tattoos, through to more recent automatic identification (auto-ID) techniques such as smart cards and biometrics. Data was collected primarily through qualitative document analysis, and the paper contains thick description typical of a narrative. The findings indicate that identification techniques born for one purpose have gradually found their way into alternate applications, and in some instances have been misused altogether. There is also strong evidence to suggest that governments are moving away from localized identification schemes to more global systems based on universal lifetime identifiers (ULI).

Keywords: identification, national identification, automatic identification, smart card, biometrics, history, government

1 Introduction

This paper takes the reader through a historical tour of identification techniques from ancient times to today. The histories shed light on how the purpose of citizen identification has changed. Its primary objective is to provide a thorough exploration of past and present government-related citizen ID schemes so as to better understand the possible uses (or misuses) of current and future mandatory ID. The paper also presents some of the evolutionary changes that have taken place in the nature and scope of citizen ID, and their subsequent potential implications on society. Historically governments have requested the registering of their population for census collection and more recently the need to know what social benefits accrue to each household but today citizen ID schemes are even used to open bank accounts. In addition, auto-ID techniques are not only pervasive but are increasingly becoming invasive. The significance of this paper is in its capacity to draw examples from history and to emphasize the types of issues that should be carefully deliberated in the introduction of any new national ID-based scheme. These schemes need forward planning and safeguards beyond those currently provided.

2 Defining identification

Identification is defined as “the act of identifying, the state of being identified [or] something that identifies one” [1]. The verb *identify* is linked to the noun *identity*, such as in the case of the term *identity card* which can be used to identify someone belonging to a particular group. Founded in Europe the word *identity* became noticeable in the English-speaking world around 1915 through Freud. The preferred definition for *identity* within the context of this paper is the “condition, character, or distinguishing features of person or things effective as a means of identification” [1].

3 Early identification techniques

Before the introduction of computer technology the various means of external identification were greatly limited. The most commonly used method was relying on one’s memory to identify the distinguishing features and characteristics of other humans, such as their outward appearance or the sound of their voice. However, relying solely on one’s memory had many pitfalls and thus other methods of identification were introduced. These included marks, stamps, brands, cuts or imprints engraved directly onto the skin, which were to be later collectively referred to as tattooing. A tattoo is defined as “...permanent marks or designs made on the body by the introduction of pigment through ruptures in the skin...” [2]. Tattooing is considered by some to be the human’s first form of expression in written form. “All the nomadic peoples try to distinguish themselves from the rest, to make themselves unique and also to establish a means of recognizing their kinsmen in the various clans. In order to achieve this, they resort to the resource which is the most accessible and the most lasting: their skin. This decorated skin defines the boundary against the hostility of the outside world, for it is visible to everyone and it accompanies the individual everywhere” [3].

Historical records date the first tattoo about 2000BC to Ancient Egypt, though there is evidence to suggest that tattooing was introduced by the Egyptians as early as 4000BC [4]. Tattoos on humans were considered both disapprovingly, and in some instances which were not lacking, quite acceptable. In the *Old Testament* in the Book of Leviticus 19:28, God commands Moses: “You shall not make any cuttings in your flesh on

account of the dead or tattoo any marks upon you". Similarly in the *New Testament* in the Book of Revelation 13:16-17, there is the infamous passage about the beast who forces everyone "…both small and great, rich and poor, free and slave, to receive a mark on their right hand or on their foreheads, and that no one may buy or sell except one who has the mark…" [5] In classical literature however, tattooing served to identify the bearer's rank, status or membership in a group or profession. The historian, Herodotus (c. 484 BC - c. 425 BC) writes concerning the Thracians, "[t]hey consider branding a mark of high birth, the lack of it a mark of low birth" [6]. The mark was usually visible for others to recognize.

3.1 The misuse of manual identification techniques

Branding as a method of identification (especially of minority groups) continued throughout history. As far back as antiquity tattooing was generally held in disrepute, "[t]he ancient Greeks branded their slaves (*doulos*) with a delta, and the Romans stamped the foreheads of gladiators, convicted criminals sentenced to the arena, for easy identification" [4]. According to Paoli, "…the Romans fastened to the necks of slaves who were liable to run away an iron collar with a disc (bulla) firmly attached to it bearing the owner's name and address" [7]. Even until 1852, the French penal system would identify thieves by "...a V tattooed on the right shoulder, and galley slaves by the three letters GAL" [3]. United States convicts and British Army deserters were similarly treated.

In recent times however, society has become intolerant of tattooing as a means of enforced segregation where the act is committed without the permission of the bearer, with dubious intent. Nazi dictator Adolf Hitler in his planned genocide of the Jewish people during World War II (1939-1945) enforced various methods of identification to separate them from the rest of the population. There is even evidence to suggest that punch cards originally intended to help in the tabulation of census data, were used instead to help segregate the Jewish people from the rest of the German and Polish populations [8]. On September of 1941, an order was issued that all Jews were to wear a Star of David badge [9]. Those who did not comply with such orders were sent to Nazi extermination camps immediately where they were "...branded like animals. A

registration number, corresponding to the camp, was stamped on the left forearm. This was preceded with a “D” if the person was Jewish...” [3]. In the *Drowned and the Saved*, Primo Levi, an Auschwitz survivor, writes of the mandatory tattooing of individuals that occurred in the concentration camp: “...a true and proper code soon began to take shape: men were tattooed on the outside of the arm and women on the inside; the numbers of the Zigeuner, the gypsies, had to be preceded by a Z. The number of a Jew, starting in May 1944... had to be preceded by an A, which shortly after was replaced by a B... After this date, [September 1944] there began to arrive entire families of Poles... all of them were tattooed, including newborn babies” [10].

In this case both the character and the number were used for identification. The character indicated the group the individual was linked to and the number uniquely identified the individual. Another survivor was quoted in *The Nazi Doctors: medical killing and the psychology of genocide*, “I remember when… that thing [the number tattooed on each prisoner’s forearm] was put on…” [11]. That *thing* according to another account stood for dehumanization. “And as they gave me my tattoo number, B-4990, the SS man came to me, and he says to me,| “Do you know what this number’s all about?”| I said, “No, sir.”| “Okay, let me tell you now. You are being dehumanized” [12]. Even until the fall of communism, the former Soviet Union used branding methods on exiled criminals and political prisoners in Siberia, for security purposes [13].

Of course the wearing of a badge does not immediately imply misuse- it all depends on the context and who it is that has requested this manner of identification and for what purpose. For instance, European migrants in the early 1900s travelling by ship to New York City were given a badge to wear to make identification easier while going through immigration. The badge was either pinned on clothing or as in the majority of cases tied to a cotton necklace. After undergoing a medical examination certain letters would be recorded on the badge to identify the condition of the immigrant, especially if further screening was required. Those suspected of suffering from mental illness or other health concerns not acceptable to authorities were separated from larger groups and sent back to their homeland. There was simply no other manner in which hundreds of thousands of people could be processed efficiently in such a short period. The badge

also alleviated the requirement for the migrant to communicate with officials, especially because the majority did not know English and this would have been a cumbersome process.

One can see that the early identification techniques, while primitive in nature, could be hideously misused against minority groups in helpless situations. Plainly, when a technique becomes available it is applied wherever it is required, “without distinction of good or evil” by whomever has the capability and authority [14]. Ellul believed that the technique itself has an autonomous mandate, that “…once man has given technique its entry into society, there can be no curbing of its gathering influence, no possible way of forcing it to relinquish its power. Man can only witness and serve as the ironic beneficiary-victim of its power” [15]. That being true, advances in data collection techniques have even greater far-reaching effects.

4 Advances in record-keeping

As manual record-keeping procedures evolved, identification became an integral part of the data collection process. Widespread branding of people was unacceptable and thus other means had to be developed to allow authorities to keep track of individuals. These means varied throughout the ages but increased in sophistication especially after the Industrial Revolution. When automation occurred most of the manual techniques were ported into an electronic environment. The following section is meant to shed light on some of the incremental innovations that led to the development of automatic identification.

4.1 The registering of people and the census

The registering of people dates back to ancient times. “Now go throughout all the tribes of Israel, from Dan to Beersheba, and count the people, that I may know the number of the people” (2 Samuel 24:2; rf 1 Chronicles 21:1,7; Esther 6:1). And the Romans were particularly advanced in their data collection requirements, wishing not only to count but to gather additional information about their citizens: “A periodic census of Roman citizens was held… every four years, but from 209 BC onwards… every five years… This was a reflection of the mustering of

the army into centuries, and it was these men, grouped in the five classes, that were the chief concern of the censors who had to register them in their tribes and assess their property in order to assign them to the correct classes for purposes of both taxation and military services. The head of each family had to answer questions about the property and age of all its members…" [16]. Consider also Luke 2:1-3: "And it came to pass in those days that a decree went out from Caesar Augustus that all the world should be registered. This census first took place while Quirinius was governing Syria. So all went to be registered, everyone to his own city."

Censors had to rely on manual identification techniques to ensure the accuracy of inventories. This was a very difficult and time-consuming task, especially since "…houses had no numbers, and many streets were nameless. The ancients had not discovered the countless practical advantages of numbers" [7]. An error made by the censor could impact the life of a citizen since "early inventories were made to control particular individuals- for example, to identify who should be taxed, inducted into military service, or forced to work" [17]. Over time however, newer more advanced techniques were developed which ultimately served to change the purpose of the population census. However, it should be noted, that "[s]trictly speaking, the modern population census began in the 17th century. Before then, inventories of people, taxpayers, or valuables were made; but the methods and purposes were different to modern ones" [17]. More automated means of identification and data collection made it possible for census surveys to be extended. For example, in the U.S. Census of 1890, part of the process of classifying and counting the data collected was automated. Herman Hollerith invented a method that allowed census takers to punch holes in predetermined locations to represent various characteristics. The holes were then processed by a machine. As elementary as this may seem, such advances led to subsequent breakthroughs in the field [18]. Of course, this does not mean that errors in the data collection of personal information are no longer incurred.

4.2 Record-keeping by the Church and State

The overall intent of a census was to determine the aggregate profile of people residing within a defined geographic region so that authorities

could address their needs appropriately. “Census statistics are used as the basis for estimating the population at the national, state and local government levels, for electoral purposes and the distribution of government funds. They are used by individuals and organizations, in the public and private sectors, for planning, administration, research, and decision making” [19]. However with advances in social welfare, authorities required to know more specific details about their citizens and their individual circumstances. In establishing an official relationship with the citizen, identification and specialized record-keeping practices became important from the perspective of the state. A variety of paper-based documentation was instituted; in some cases special seals or ink-based stamps were used to indicate legality. Examples of official documentation included land title deeds, birth certificates and bank account records. These were among the most common proofs of identity but this varied dependent on the state in question and period of history. The importance of the church in the evolution of record-keeping should also be highlighted. In many parts of the world the local church was a thorough documenter of events and very much an integral part of government until about the Middle Ages. The church and state had their own law and court systems and there were often issues over jurisdictional rights [20,21]. The interaction of the church and state led to developments in the centralization of government and bureaucracy. With the centralization of power came a need for the centralization of citizen information which led to the creation of personal files. Churches also provided proofs of identity, such as marriage and baptismal certificates. Some churches even kept records of disputes or wrong-doings and how victims had been recompensed. Given that the size of towns was relatively small compared to today, names could be used to identify individuals. Given names and surnames were not always unique. In some instances the name was accompanied by the paternal lineage, or an address location, or by a nickname. However even address locations in ancient times were for the greater part difficult to precisely identify. In ancient Rome, roads were nameless “and were referred to simply by such expressions as ‘The road to…’; a few of the more important had names” [7]. But the Industrial Revolution was set to change things dramatically, especially as mass production drew large groups of people (in most cases

from surrounding towns) closer towards employment opportunities in factories.

4.3 The notion of a personal document file

One of the earliest modern day responses to improved identification techniques and record-keeping standards came in 1829. In that year, British Parliament made a decision to enact the reforms of Prime Minister Robert Peel who wanted more emphasis to be placed on printed police records. In this manner relevant data could be stored in a personal document file and linked back to individuals using a unique value. In many ways these records were forerunners to government databases that were linked to ID cards. During this same period, photographic technology was invented but it was not until 1840 that amateur scientist William Henry Fox Talbot developed the negative-positive photographic system which eventually became a useful police identification tool. In an age of computers, humans generally take for granted the invention of the still-shot camera and motion camera because the technology is so readily available. But a simple ID badge with a photograph on it really did not become widespread until after the Second World War. Photographs fastened to cards were excellent manual identifiers, before the proliferation of cameras which then enabled fake IDs to be developed by criminals. As soon as this occurred an additional measure was required to ensure positive identification. In the meantime, signatures were the most reliable unique method of cross-checking someone's identity between original and duplicate copies. This was all dependent on the literacy level of the individual, though unique markings were accepted as substitutes. By the late 1870s, a significant breakthrough in identification came about in India. Sir William Herschel (a British 'Magistrate and Collector') had made a defendant's fingerprint part of court records. Ron Benrey reported that Herschel used fingerprints as manual signatures on wills and deeds [22]. For the first time, a biometric had officially become a means of precise identification. In 1901, police technology had advanced so much that Scotland Yard had introduced the Galton-Henry system of fingerprint classification [23]. Till today, fingerprints have been associated with crime for this reason. The system did not become widespread because the practicality of taking fingerprints of all citizens and cross-matching records

for individual transactions was not viable at the time.

4.4 The evolution of the citizen ID number

Unique citizen identification numbers were adopted by numerous countries around the period of the Great Depression. Unique identifiers in the context of citizen numbers are known by a variety of names. These include: identification number (IN), personal identification number (PIN), uniform personal identification mark (UPIM), national identification number (NIN), universal identification number (UIN), unique identification system (UIS), universal identifiers (UID), unique personal identifier (UPI), single identifying number (SIN), standard universal identifier (SUI), universal multipurpose identifier (UMI), universal personal number (UPN), unique lifetime identifier (ULI). The majority of these nation-wide numbering schemes have been maintained, relatively unchanged, till today. Some of the national numbering schemes include: the Person Number (PN) system of Norway, the Central Register of Persons (CRP) in Denmark, the German Insurance Number (GIN), the Social Account Number (SAN) of Austria, the Insurance Number (IN) of the former Czechoslovakia, the French Identification Number (FIN), the Insured Persons Number (IPN) of Switzerland and the National Insurance Number (NIN) of the United Kingdom [24].

The initial person registration system used in Sweden dates back about three hundred years when the process involved the Church of Sweden. Local parishes were considered to be like regional administration offices. But in 1947 each person was assigned a PN that was recorded electronically in 1967 from metal plates to magnetic tape. The Netherlands used the census of 1849 as a starting point for there decentralized PN system. But in 1940 personal cards with unique numbers were issued to the whole population that acted as lifetime identifiers. In Israel a PN was allotted in 1948 via a census after the State of Israel was officially established. A Population Registry Law in 1965 established the basic information that had to be collected when registering. This involved disclosing details about the ethnic group that one belonged to, as well as religious beliefs and past and present nationalities. In 1966, this information was computerized. Iceland has used a population register since 1953. When a citizen reaches the age of twelve they are given a number that is based on the alphabetical

sequence of a person's name in the total population. In 1964, Norway's Central Bureau of Statistics was asked to establish a national identification numbering system as the world learnt of the potential of electronic data processing (EDP). In 1968, Denmark followed in Norway's footsteps by computerizing their records as well. France has used numbering systems for individuals and organizations since 1941. The system was computerized in 1973 after existing records were put on magnetic tape and adapted to include check digits. Finland introduced their personal identification code (PIC) system in 1964 [25]. The potential for a globally implemented unique national identifier (UNI) is realistic. This could be tied in with the concept of a follow-me telephone number such as that defined in Universal Personal Telecommunications (UPT). UPT "…will enable each user to participate in a user-defined set of subscribed services and to initiate and receive calls on the basis of a personal, network-transparent UPT Number across multiple networks and any terminals, fixed or mobile, irrespective of geographic location limited only by terminal and network capabilities and restrictions imposed by the network operator" [26]. For the purpose of showing the evolution of the citizen ID number, one of the oldest schemes, the United States social security number (SSN), will be discussed in more detail. The maturation of the SSN is representative of many person number schemes worldwide.

5 The U.S. Social Security Administration (SSA)

By the 1920s, countries like Britain, Germany and France were using personal document files to administer specific government assistance schemes for unemployment, worker's compensation, health, pensions and child endowment [27]. Western European countries had established population registers that were updated continually to include the name, residence, age, sex and marital status of an individual. The registers were administered at a municipal or county level initially but towards the mid-1900s they became more centralized. There was an increasing demand for the registers by government for voting, education, welfare, police and the courts. In observing the processes of the European governments, the United States (U.S.) sought even more efficient methods of identification. Thus the Social Security Administration (SSA)

was formed, a centrally managed scheme, supported by an official Act in 1935. Setting up the program was a daunting task. The U.S. government was dealing with a large group of people (five million elderly people alone), each personal record attached to several applications (pension, medicare, family allowance etc.), and individuals were geographically dispersed. Since money and benefits were being distributed at a cost to taxpayers, the government was obligated to establish guidelines as to eligibility, proof of identity and citizenship to keep track of funds [28].

5.1 The SSN gathers momentum – more than a number

As government policies became more sophisticated, administrators required a mechanism for the unique identification of individuals to improve the efficiency of operations. In 1938 the social security number (SSN) was introduced. The SSN was phased in to reduce the incidence of duplicate records, allow for more accurate updates and ensure that entitlements were received by the bona fide. With the introduction of the SSN came the social security card. Each card contained the nine digit SSN and the cardholder's name. The card (with the printed number on it) was useful in that cardholders could carry it with them and quote it freely when requested to fill out government forms. It meant that citizens did not have to memorize the number or risk referencing it incorrectly. The card also acted as a proof of identity. This deterred many people from making fraudulent claims, yet the quality of the paper card was poor and susceptible to damage. Thus the need for cards to be made out of more durable material ensued. Cards made out of cardboard were initially introduced, followed by plastic cards with embossing. By 1943, President Roosevelt had signed "...Executive Order 9397 (EO9397) which required federal agencies to use the number [SSN] when creating new record-keeping systems" [29]. In the early fifties the insurance and banking sector also adopted the SSN and requested it from each individual who wanted to open a bank account and make monetary transactions. By 1961, the Internal Revenue Service (IRS) was also using the SSN as a taxpayer identification number (TIN). It can be seen that knowledge gained from the improved administration of government services was applied to other sectors, such as finance. Thus the ID number itself, had two important uses when the computer age arrived.

First it could be used as a primary key for storing personal information in databases. Second it could be linked with any identification technique for authentication or verification. It was the ID itself that was fundamental to these applications whether in the form of a unique number, character set, symbol or image. The ID device accompanying the ID was more a facilitator. What should be observed is that even without advanced hardware equipment and automatic identification techniques, the underlying information systems concept had been born.

5.2 The computerization of records

The proportion of recorded transactions was now reaching new limits in the United States. Written records had served their purpose but could no longer effectively support the collection, storage and processing of data. Government agencies were plagued by such problems as limited physical storage space for paper documentation; slow response times to personal inquiries; inaccurate information stored in personal records; difficulties in making updates to records; duplicate information existing for a single person; and illegal and fraudulent claims for benefits by persons. By 1970 the SSA had set up its headquarters in Baltimore. The basic data stored there included the "...social security status of every citizen with a social security registration... and equivalent records on all phases of the Medicare program." The SSA had established 725 field offices and citizen transactions were communicated to headquarters via dedicated circuits where it was received on magnetic tape ready for input into the SSA computer [30]. Initially, the types of analysis that could be performed on records were limited [31]. By 1977 however, the government had not only computerized its paper records but had even developed computer matching applications. The Public Law 95-216 "mandated that state welfare agencies use stage wage information in determining eligibility for Aid to Families with Dependent Children (ADFC). Subsequent legislation also required similar wage matching for the Food stamp program" [32]. By the early 1980s it was common for data matching programs to check personal records between social security, other federal agencies and the banking sector. In this manner the government could determine whether a citizen was receiving legitimate funds and contributing to the nations numerous taxes. Thus, the emergence of the microprocessor and the

development of electronic storage devices enabled the invention of information technologies that could automate the process of identifying living and non-living things [33]. Historically, auto-ID systems have been constrained by the capabilities of other technologies they have been dependent upon. Limitations in network infrastructure, central processing unit (CPU) speeds, electronic storage space, microchip miniaturization, and application software and data collection devices are just some of the components that have impacted auto-ID. For example, it has already been noted in this chapter that the first biometric manually recorded for criminal records was the fingerprint as far back as the 1870s. However, it took more than one hundred years to develop a commercial electronic fingerprint recognition system that had the ability to store thousands of fingerprint minutiae and cross-match against a large database of records with a workable response time.

5.3 Problems with some government citizen identifiers

The U.S. social security number ultimately became a multi-purpose identifier though originally it was only meant to be used for social security purposes. As paper records were transferred into a machine-readable format and simple searches performed it became apparent that there were duplicate SSNs. One must note that the SSN was created without the knowledge of how computer technology would revolutionize the government's processes. By the time computers and networks were introduced into the SSA's practices, the SSN was a legacy system that maintained numerous embedded problems. The main cause for concern arose because the identifier's composition was never well-defined; neither was it randomly or sequentially generated. The nine digit SSN was broken up into three sections: area number assigned to states on a population basis, group number (2 digits), and serial number assigned sequentially (4 digits) which was controlled by the first six letters of the person's surname [24]. When the regional-based ID numbers were pooled together to form a central population register (CPR) the IDs were found not to be unique. As Hibbert critically points out, "[m]any people assume that Social Security numbers are unique, but the SSA didn't take sufficient precautions to ensure that it would be so" [29]. In addition to this, the SSA itself was forced to admit that more than four million people had

two or more SSNs [34]. This immediately posed a problem for both authorities and citizens. The computer system could not handle cases adequately whereby there were more than 999 persons with a surname beginning with the exact same 6 letters living in the same area (as defined by the SSA). While this may sound impossible to achieve some names are very common and a lot of surnames are shorter than 6 characters in length. In other cases the problems that some citizens have endured after their SSN has been stolen, have been well-documented and receive plenty of attention from popular media. The call for some other means of identification, automatic in nature, was heeded and many states more recently have acted to implement state-of-the-art biometric and smart card-based systems to alleviate issues of duplication and crime. The rest of the world have followed the U.S. example, more recently even those countries considered as either lesser developed (LDC) or newly industrialized countries (NIC).

6 The rise of automatic identification techniques

6.1 The commercialization of identification

New technological innovations originally intended for government often find themselves being applied commercially within a short period of time. The lessons of the SSN and other early identification systems were used to improve processes in banking and retail from the 1970s onwards, as a variety of auto-ID technologies became available to implement. The introduction of the bar code and magnetic-stripe card especially was noticeable because it directly impacted the way people shopped and banked. Consumers now had the ability to withdraw funds without having to visit a bank branch. Shop store owners could use bar codes on products to improve their inventory control and employ fewer workers because of the speed of checking-out items. These innovations were not only targeted at what one would term mass market but they affected every single person in the community; the bar code was linked to the purchasing of food and other goods, the magnetic-stripe card to money that is required for survival in a modern society. And as one scientist wrote in 1965 “...the impact of automation on the individual involve[d] a

reconstruction of his values, his outlook and his way of life" [35].

6.2 Too many IDs?

As government and enterprise databases became widespread and increased in sophistication, particularly after the introduction of the desktop computer in 1984, implementing auto-ID solutions became possible for even the smallest of businesses. Auto-ID could be applied to just about any service. The vision of a cashless society gained momentum as more and more transactions were being made electronically and the promise of smart cards was being publicized. But instead of wallets and purses becoming thinner since the need to carry cash was supposedly diminishing, the number of cards and pieces of identification people had to carry increased significantly. Citizens were now carrying multiple devices with multiple IDs: ATM cards, credit cards, private and public health insurance cards, retail loyalty cards, school student cards, library cards, gym cards, licenses to drive automobiles, passports to travel by air and ship, voting cards etc. Dependent on the application and the auto-ID device being used, passwords were also required as an additional security measure. But since passwords such as Personal Identification Numbers (PINs) were never meant to be recorded, expecting consumers to remember more than one PIN was cumbersome. But as Davies pointed out, while "[m]anaging all these numbers is a chore… it's a state of affairs most of us have learned to accept" [36]. This statement was probably an interim truism until the turn of the 21st century. Today, more than ever, most likely due to major technical breakthroughs, there is an underlying view that computers are supposed to make life less complicated rather than more complicated. The vision is still one where cards (probably multiapplication and multifunctional in nature) will play an important role in identification but whereby other advances such as biometric recognition systems will be an integral part of the solution to ID.

6.3 Numbers everywhere

In his book, *Rome: its people, life and customs*, Ugo E. Paoli (1990, ch. XIII) emphasizes the significance of numbers by describing what it was like in ancient Roman times without street addresses. He contrasts this

setting, i.e. the streets without names and the houses without numbers, by referring to how numbers are used profusely today in modern civilization. It is worth quoting Paoli at length [7]:

> "[w]hen we travel, our train has a number, as do the carriages, the compartments, the seats, the ticket-collector, the ticket and the note with which we buy our ticket. When we reach the station we take a taxi which is numbered and driven by a driver similarly numbered; on arrival at our hotel we become a number ourselves. Our profession, age, date of arrival and departure are all reckoned in numbers. When we have booked a room, we become a number, 42 perhaps, and if we are so unfortunate as to forget our number we seem to have forgotten ourselves. If we mistake it, we run the risk of being taken for a thief, or worse. The number is on the disc hanging from the key in our room; it is above the letter rack in the hall; every morning we find it chalked on the soles of our shoes, and we continually see it on the door of our room, and, finally, we find it on the bill. We grow so used to our number that it becomes part of us; if we have a parcel sent to the hotel, we give the number 42; however important we may be, to the porter and the chambermaid we are simply No. 42."

Everything is indeed numbered. Even we ourselves are numbered. And as Paoli continues, this great ease in identifying everything is supposedly "a result of our position as modern civilized men" [7]. These ubiquitous ID numbers (which include addresses) follow us everywhere, and not unexpectedly as Paoli also reckons, have almost become a part of our personalities. On extending this notion Paoli reminds us that even if one finds themselves homeless, without an income, without any hope for the future, they still have their ID number. In a similar light what should be underscored is the increasing requirement today towards obligatory practices to do business with one's ID number(s). Whether making a transaction over the counter, through the mail, or on the telephone, service providers have become more interested in our customer reference number than our name. One is led to a justifiable conclusion of whether in amongst all these manufactured numbers we are little by little, losing our natural right to be called by our given name, and hence allowing for the defeat of our identity.

7 Mandatory ID with modern technologies

In the U.S. biometrics systems have been used for electronic benefits transfer (EBT) and other social services, since July 1991 [37]. In a bid to stop fraud, the Los Angeles County in California introduced AFIRM (Automated Fingerprint Image Reporting and Match) for the administration of its General Relief (GR) program in the Department of Public Social Services (DPSS). GR is for people who are not eligible for financial assistance from both the federal and state governments. In 1994, National Registry Incorporated (NRI) supplied finger-image identification systems to the Department of Social Services (DSS) in Suffolk County and Nassau County, New York. The New Jersey Department of Human Services and DSS of Connecticut were also later clients of NRI- all requiring finger-image systems to eliminate fraudulent activities. David Mintie, the project coordinator of Digital Imaging for the state of Connecticut, reported that this electronic personal ID system: “conveniently and accurately enrols qualified General Assistance (GA) and Aid to Families with Dependent Children (AFDC) clients into a statewide database; issues tamper-resistant identification cards that incorporate finger-image ‘identifiers’ stored in two-dimensional bar codes; uses finger-image identification to verify that enrolled clients are eligible to receive benefits” [38].

Also in 1995, the San Diego Department of Social Services (DSS) announced that it was implementing a pilot project for a fingerprint identification solution to ensure that public funds were being distributed to the correct recipients. Among the problems of the legacy system outlined by the county supervisor were the falsification of photos, signatures and social security numbers which were encouraging applicants to sustain multiple identities (commonly referred to as double-dipping). In November of 1996 the Pennsylvania DPW issued a Request for Proposal (RFP) for an automated fingerprint identification system (AFIS). As Mateer of BHSUG reported, the system referred to as PARIS (Pennsylvania Automated Recipient Identification System) will “capture digitized fingerprint, photo, and signature images of cash, food stamp, and medical assistance ‘payment name’ recipients, who are required to visit county assistance offices (CAOs)” [39].

In 1996 in Spain, all citizens requiring to be considered for

unemployment benefits or worker's compensation were issued with a smart card by the Ministry of Labor and Social Security [40]. The so-named TASS (Tarjeta de la Seguridad Social Espanola) initiative requires the fingerprints of the smart card holder. Unisys reported that by early 1997 about 633 kiosks would have been installed in eight cities of the Andalucia region, covering about one fifth of Spain's total population (i.e. approximately 7 million persons). The TASS project has brought together some of the biggest telecommunications manufacturers, like Motorola (IC), Fujitsu-Eritel (network infrastructure), AT&T (kiosks), Siemens Nixdorf (smart card reader/writers) and Telefonica Sistemas (portable reader/writers). Similarly the Dutch National ChipCard Platform (NCP) requires the cardholder's personal and biometric data to be stored on a smart card "…and be readable across a wide variety of terminals- for instance at libraries, banks, insurance companies, theatres, municipal authorities and mass transit undertakings" [41]. Cambodia's national identification card also stores biometrics (fingerprints) but on a 2-D bar code instead of an integrated circuit.

INSPASS is envisioned to grow to include other airports at Miami Chicago, Honolulu, Houston, Los Angeles and San Francisco. Old sites at JFK, Newark, Toronto and Vancouver are being upgraded with the latest technology. The focus will be to replace hand geometric devices with fingerprint devices in the long-term to ensure standardization. In 1996, the German federal government was seeking to implement hand geometry at the Frankfurt's Main Airport. The preferred German biometric technology was hand geometry which differed to that biometric used in the INSPASS project at Newark, JFK and Toronto airport. The U.S. and Canada are not the only nations that are working on automated inspection systems for immigration purposes. In 1996, others countries included Australia, Singapore, Hong Kong, Holland, Germany, and the United Kingdom, Bermuda. Travelers who would like to be identified using biometrics have to undergo a profile security check by authorities. In the case of North America, this includes checking whether the traveler is a permanent resident or citizen of the U.S., Canada, Bermuda or part of the Visa Waiver Pilot Program (VWPP), has a criminal history or any previous customs infringements. If the traveler is deemed to be of low risk, they are enrolled to use the system for one year- the pass must be renewed

annually. Only PortPASS holders are required to pay a small fee to enrol. When INSPASS began there were only 2000 frequent fliers, by 2000 there were over 100000.

7.1 Towards integrated auto-ID applications

In the past, governments worldwide have been criticized for their inefficiencies regarding the distribution of social services. There are still many developed countries around the world which use paper-based methods in the form of vouchers, coupons, and ration cards, concession cards to operate large-scale federal and state programs. As recent as 1994, even the Department of Agriculture in the U.S. issued paper coupons for food stamp programs, however, it was not long before they moved to an electronic system [42]. Since that time, the U.S. also introduced 'food card' applications using magnetic-stripe (Pennsylvania-since 1984) and smart cards (Ohio since 1992). Some states used magnetic-stripe cards to help verify that the patient was indeed eligible for 'free' consultations to the doctor. The magnetic-stripe card first replaced paper-based records that were prone to error. Smart cards are also being increasingly promoted by government agencies, many of them set to store citizen biometrics for additional security purpose. The latest trend in Federal and State government systems is program centralization [43]. Using database matching principles and smart card technology, one card can be used to store all the citizen's personal information as well as their eligibility status to various State programs. The single card approach not only greatly reduces operational costs but is equipped to catch out persons who have deliberately set out to mislead the government. In the U.S. for instance, there is a new Electronic Benefits Transfer (EBT) paradigm which calls "for a single card that can deliver benefits from multiple government programs across all states... federal planners hope the entire country will be under the new system by 1999" [44]. The initial focus is on food stamps and AFDC but other benefits such as old-age pension, veteran survivors, and unemployment will eventually be integrated into the system [45].

Singapore, Spain, Germany and the Czech Republic were some of the first countries to introduce national ID smart cards. One of the largest-scale smart card government projects is in China, led by China

Citizen Card Consortium. The plan is to have one integrated card for citizen identification, health care and financial purposes. “The smart card is set to store the bearer’s ID number, health care code, address, birth date, parents’ names, spouse’s name and a fingerprint” [46]. The Taiwan government is willing to learn from this Chinese initiative as their own paper-based identification card was extremely ineffective- it did not carry a magnetic-stripe, nor did it have embossed numbers and it was very flimsy. The Philippines government is also embarking on a national ID card project which will include biometric data as are the South Africans with the Home Affairs National ID System [47]. Malaysia and Thailand are also following in the footsteps of Singapore. In 1998 in South America, there were smart card trials in Brazil (Curitiba) where 30000 city employees were issued with smart cards that acted as a government ID and allowed monetary transactions. In 1999, the program was extended to the families of employees, and then to the city’s entire 1.5 million urban population. This ID card has an RF interface, i.e. it is contactless. More recently, Saudi Arabia has embarked on a national ID scheme.

The U.S. Department of Defence (DOD) instituted a multiapplication smart card to replace the various military paper records, tags and other cards. The MARC program (Multi-Technology Automated Reader Card) was a targeted pilot in the Asia Pacific with 50000 soldiers. According to authorities, it was so successful that the card was distributed to all 1.4 million active duty armed forces personnel. Many believe that MARC was a large-scale trial necessary to prove-in a national ID for all citizens in the U.S., incorporating numerous government programs. Coordinator, Michael Noll said that the ultimate goal of MARC was: “[a] single standard, multiple-use card that [could] be used across the government... for applications such as payroll, employee records, health care and personnel assignments” [48]. MARC was first used during the Gulf War crisis. The card contains a magnetic-stripe and integrated circuit, as well as a photograph and embossed letters and numbers and it can handle up to 25 applications. Like the U.S., Singapore is also presently testing a military ID card. The Clinton Administration also wanted to adopt smart card technology to track the expenses of federal government staff, responsible for 8.5 billion US dollars of annual expenditure. The card would be used to log travel expenses, make small purchases and allow

for building access [49]. Also, smart cards may be the driving force behind digital signatures allowing for encrypted messages between government agencies and citizens.

8 Post Sept 11- the changing face of ID

In the United States, after the terrorist attacks of Sept 11in 2001, several bills were passed in Congress to allow for the creation of three new Acts related to biometric identification of citizens and aliens- the Patriot Act, Aviation and Transport Security Act, and the Enhanced Border Security and Visa Entry Reform Act. Many civil libertarians were astounded at the pace at which these bills were passed and related legislation was created. The USA has even placed pressure on international travellers and their respective countries to comply with biometric passports or forgo visiting altogether. To some degree national security measures are moving from a predominantly “internalized” perspective to an outward-looking view. With this change has been a re-shaping of nation-specific requirements for citizens both in-country and outside its borders to comply with obligatory conditions. For example, in 2002 Britain announced plans to chip implant illegal immigrants to control migration, and in 2003 Singapore seriously considered electronic tagging for persons suspected of carrying the deadly Severe Acute Respiratory Syndrome (SARS).

Heightened national security sensitivities have meant a reorganization of our priorities and values, especially when it has come to identification. It seems we have now become obsessed with identifying as a means to providing additional security, as if this is the answer to national security. This is not to say that clear advantages do not exist in the use of automated systems. For example, in 2004, unidentified Tsunami victims who lost their lives in Thailand were actually fitted with RFID chips so that their loved ones might have been able to identify them later [50]. But by and large governments are now introducing sweeping changes to citizen ID systems without considering the probable repercussions into the future.

What started out as a need to identify individuals *within one’s borders* has now evolved into a national-wide scheme and is poised to make a

debut as an international-based solution. Blocks forming like the European Union with a single currency are potentially the first test-beds for the larger scale ID schemes. Livestock in EU countries for example are currently being identified uniquely based on a common standardized approach described in a legislative directive. The question to ask, however, is who can ensure that current and future schemes are not misused by any ruling individual or power base. While automatic identification schemes offer convenience, speed, higher productivity, better accuracy and efficiency, they are in their very nature “controlling” techniques- they either grant access or deny it. History has shown what was possible with largely manual-based techniques during WWII, auto-ID techniques at the disposal of a similar head of state could be manifold more intrusive. One need ask now, what safeguards have been put in place to prevent the misuse or abuse of one’s personal ID? Some auto-ID technologies even pose legal dilemmas. One could claim that biometric techniques for instance, and beneath-the-skin RFID transponders, do encroach on an individual’s privacy when used for ID. Biometrics like fingerprints or DNA are wholly owned by the individual yet requested and stored by the state on large citizen databases.

While in today’s society the need for ID is unquestionable, we need to ensure we do not enforce changes that are irreversible and perhaps even uncontrollable. While national ID schemes were introduced by a number of countries after the Great Depression of the 1930s, what has changed since their inception are the technological capabilities that we have at our fingertips. These auto-ID technologies are manifold more powerful and when enjoined to other automated processes are a magnitude more invasive. The periodic census is a fine example of something that was introduced by the church and state to collect data in order to help provision services for citizens. Today, however, aggregated census data is being sold as a commodity to help private organizations perform more precise “target marketing”. Perhaps it is not too long before our “private” IDs also undergo a similar transformation- “DNA for sale, anyone?”

9 Conclusion

Tracing the path from manual identification through to automatic

identification some conclusions may be drawn. First, the practice of identification has been sourced to very ancient times. Second, throughout history manual ID of humans was not always a voluntary modus operandi, especially in the enforced tattooing of individuals by some extreme groups. Third, the identification processes and procedures that were developed before automation were replicated after automation and dramatically enhanced because computer technology allowed for more powerful processing of information. Legacy systems however did impact automation. Fourth, the success of auto-ID was dependent on the rise of information technology. In many ways auto-ID was limited by a variety of hardware and software system components. As soon as these became feasible options for service providers, both in affordability and usability, auto-ID flourished. Fifth, the widespread adoption and acceptance of auto-ID by citizens is indicated in that people carry so many different ID devices for different applications. And finally, and most importantly, national ID schemes are becoming increasingly pervasive, complemented by highly invasive technologies. Governments need to be forward-thinking when they introduce new schemes and/or new devices, or extend existing schemes to new application areas, particularly of a commercial nature such as banking. No one can predict the future but one thing is certain, if a technology (high-tech or other) is open to misuse, it will eventually be abused.

References

[1] Delbridge, A. et al. (Eds), *Macquarie Dictionary*. Sydney: Macquarie University, 1998, p. 1062.

[2] Encyclopaedia Britannica, “Tattoo”, *The New Encyclopaedia Britannica Micropaedia*. Sydney: Helen Hemingway Benton, Vol. IX, p. 841, 1983.

[3] C. Grognard, *The Tattoo: graffiti for the soul*. Spain: The Promotional Reprint Company, 1994, pp. 19, 21, 25.

[4] T. Cohen, *The Tattoo*. Sydney: Savvas, 1994, pp. 25, 32.

[5] M. G. Michael, “The Number of the Beast, 666 (Revelation 13:16-18): Background, Sources and Interpretation”, MA (Hons) dissertation, Department of History, Philosophy and Politics, Macquarie Univ., Sydney, Australia, 1998.

[6] Herodotus, *The Histories*. London: Penguin Books, 1972, p. 282.

[7] U. E. Paoli, *Rome: its people, life and customs*. London: Bristol Classical Press, 1990, pp. 138-140.

[8] E. Black, *IBM and the Holocaust*. UK: Little, Brown and Company, 2001, pp. 22, 58.
[9] M. Kitchen, *Nazi Germany at War*. Essex: Longman, 1995, p. 202.
[10] P. Levi, *The Drowned and the Saved*. trans. Raymond Rosenthal, London: Summit Books, 1998, p. 118f.
[11] R. J. Lifton, *The Nazi Doctors: medical killing and the psychology of genocide*. New York: Basic Books, 1986, p. 165.
[12] M. Dery, *Escape Velocity: cyberculture at the end of the century*. London: Hodder and Stoughton, 1996.
[13] C. P. Jones, 'Stigma: tattooing and branding in Graeco-Roman antiquity', *The Journal of Roman Studies*, 77, 1987, pp. pp. 148-150.
[14] J. Ellul, *The Technological Society*. New York: Vintage Books, 1964, pp. 98-100.
[15] W. Kuhns, *The Post-Industrial Prophets*: *interpretations of technology*. New York: Harper Colophon Books, 1971, p. 94.
[16] H. H. Scullard, *Festivals and Ceremonies of the Roman Republic*. London: Thames and Hudson, 1981, pp. 232f.
[17] Encyclopaedia Britannica, "Census", *The New Encyclopaedia Britannica Micropaedia*. Sydney: Helen Hemingway Benton, Vol. II, 1983, p. 679.
[18] G. D. Austrian, *Herman Hollerith: forgotten giant of information processing*. New York: Columbia University Press, 1982.
[19] I. Castles, *CDATA91 Data Guide: 1991 census of population and housing*. Canberra: Australian Bureau of Statistics, 1993.
[20] C. T. Anglim, *Religion and the Law: a dictionary*. California: ABC-CLIO, 1999.
[21] R. C. van Caenegem, *The Birth of the English Common Law*. Cambridge: Cambridge University Press, 1988.
[22] Connecticut Dept. (1998, November 23). Understanding public perception, *Connecticut Department of Social Services* [Online]. Available: http://www.dss.state.ct.us/faq/disuppt.htm, pp. 1-3.
[23] H. C. Lee, and R. E. Gaensslen, *Advances in Fingerprint Technology*. New York: CRC Pr., 1994.
[24] New Zealand Computer Society, "Investigation of a unique identification system", *NZCS*, May, 1972, pp. 28-29.
[25] A. S. Lunde et al., *The Person-Number Systems of Sweden, Norway, Denmark, and Israel*. Maryland: U.S. Department of Health and Human Services, 1980.
[26] ITC, "Address note", *Proceedings ITC, 8th ITC Specialist Seminar on Universal Personal Telecommunications*, October 12-14, p. 7, 1992.
[27] C. Clark, "The advance to social security", *Realities of Reconstruction 9*, Melbourne University Press, Carlton, 1943, p. 9.
[28] SSA. (2003, March 30). Historical development, *History: Social Security Online*, [Online]. Available: http://www.ssa.gov/history/ brief.html, pp. 1-7.
[29] C. Hibbert, "What to do when they ask for your social security number", in *Computerization and Controversy: value conflicts and social choices*, (ed.) Rob Kling. New York: Academic Press, 1996, pp. 686-696.
[30] A. Miller, *The Assault on Privacy: computers, databanks and dossiers*. London:

New American Library, 1971, p. 77.
[31] B-A. Lipetz, “Information storage and retrieval” in *Scientific American*, London: W. H. Freeman, 1966, p. 191.
[32] R. P. Kusserow, “The government needs computer matching to root out waste and fraud”, in *Computerization and Controversy: value conflicts and social choices*, (ed.) Rob Kling. New York: Academic Press, part 6, section E, 1996, pp. 653f.
[33] D. B. Yoffie, (ed.) *Competing in the Age of Digital* Convergence. Massachusetts: Harvard Business School, 1997, pp. 41-110.
[34] A. F. Westin, and M. A. Baker, *Databanks in a Free Society*. New York: Quadrangle Books, 1972, pp. 396-400.
[35] H. Sacleman, *Computers, System Science, And Evolving Society: the challenge of man-machine digital systems*. New York: Wiley, 1967, pp. 36, 552-560.
[36] S. Davies, *Monitor: extinguishing privacy on the information superhighway*. Sydney: PAN Macmillan, 1996, p. 121f.
[37] J. P. Campbell et al. (1996, November 20). Biometric security: government applications and operations, *Biometric Consortium* [Online]. Available: http://www.vitro.bloomington.in.us:8080/~BC/ REPORTS/CTSTG96/, pp. 1-5, 1996.
[38] D. Mintie (1996, April 11). Digital imaging FAQ’s: Implementing a statewide biometric identification system, *The State of Connecticut- DSS* [Online]. Available: http://www.dss.state.ct.us/faq/diplan.htm, pp. 1-2, 1996.
[39] S. Mateer, “Pennsylvania Automated Recipient Identification System (PARIS)”, *Biometrics in Human Services User Group*, 1(2), p. 2, 1996.
[40] J. M. Kaplan, *Smart Cards: the global information passport*. London: International Thomson Computer Press, 1996, pp. 31f.
[41] D. Jones, (ed.), “Dutch Model for Universal Smart Card”, *Card Technology Today*, 10(2), p. 6, 1996.
[42] T. Hausen, and P. Bruening, “Hidden costs and benefits of government card technologies”*, IEEE Technology and Society Magazine*, 13(2), p. 26, 1994.
[43] W. T. Marshall, “EBT: keeping the benefits in proper balance”, *America’s Community Banker*, 6(5), pp. 10-15, 1997.
[44] G. Robins, “Reinventing electronic benefits transfer”, *Stores*, 77(6), p. 58, 1995.
[45] W. Jackson, “EBT cards for food programs get smarter”, *Government Computer News*, 15(2), pp. 1-2, 1996.
[46] E. Valles, “Smart ID cards to guarantee privacy: national card plans get underway amid anxieties”, *China News*, 7 October, p.7, 1998.
[47] J. D. Woodward, “Biometrics: privacy’s foe or privacy’s friend?”, *Proceedings of the IEEE*, 85(9), p. 1483, 1997.
[48] W. Jackson, “The MARC card gets smarter”, *Government Computer News*, 15(1), p. 41, 1996.
[49] D. Jones, “Electronic commerce in government”, *Card Technology Today*, 10(2), p. 16, 1998.
[50] J. Smith (2005, January 1). Too many corpses to count, DailyRecord, [Online].

Available: http://www.dailyrecord.co.uk

2

Social impacts of transport surveillance

Marcus Wigan[1] and Roger Clarke[2]

[1]Oxford Systematics, [2]Xamax Consultancy Pty Ltd

Abstract

The transport sector is a natural focal point for surveillance measures to combat the threat of terrorism. It is also a complex environment that offers many examples of the social impacts of contemporary surveillance.

Surveillance needs to be assessed against the standards used to justify other forms of security measures. The efficacy of many surveillance schemes, however, is in serious doubt. Justification for these schemes is commonly either lacking entirely or is unpublished and hence has not been subjected to critical evaluation.

A small set of mini-cases is presented, in order to identify social impacts of 21st century surveillance schemes that have been implemented as fear-driven responses to terrorist acts. Those impacts are argued to be seriously harmful to Australian society.

Trust is crucial to public acceptance of intrusive measures. But the absence of justification for surveillance, and of controls over abuses, is likely to see the rapid dissipation of trust, firstly in the assertions of national security and law enforcement agencies, and secondly in the politicians who have been rubber-stamping their demands.

Keywords: trust, legitimacy, intelligent transport systems (ITS), chilling effect, security, deterrence, interception, investigation, mass surveillance, object surveillance, area surveillance, location, tracking, anonymity, passport, data linkage, privacy impact assessment (PIA), smart card, traffic, electronic toll, enforcement, speed, freight

1 Introduction

The citizens of a number of countries are under threat from terrorist actions, or at least perceive themselves to be so as a result of statements made by their governments. This mixture of real and perceived threat has enabled national security and law enforcement agencies in many countries to achieve extensions to their powers, resulting in a major shift in the balance between human rights and social control. Increased surveillance and substantial spending on surveillance technologies have been conspicuous features during this phase. This paper considers the social impacts of this increase in surveillance by reference to the surveillance in transport systems.

Transport is an attractive area in which to concentrate investment in surveillance. The huge flows of people through public transport systems, airports and public spaces are subject to transport and traffic management systems. People and goods – including both dangerous goods and dangerous people, are dependent on transport to reach their destination – or their target. Moreover, large transport vehicles, in the form of ships (in Yemen), aircraft (in New York and Washington), buses (in Israel), trains (in London and Madrid), and trucks (in Iraq on a daily basis) are the means whereby criminals inflict damage and misery, and disrupt the confidence required by the community to use transport in order to go about their business and social activities.

In addition, there has been considerable investment in information infrastructure within the transport sector, under the rubric of Intelligent Transport Systems (ITS). In most cases, the justifications for the investment were originally economic or social, but the opportunities that they offer for national security purposes are now being grasped. For example, the National Centre for Intelligent Transport Systems focuses on advanced communications as a natural development of both ITS and the external needs for command, control – and surveillance.

Surveillance is, however, intrusive and demeaning. It signals that

powerful organisations distrust people, and it encourages distrust by people of one another, and of organisations (Clarke 1988). It creates a 'chilling effect' on various kinds of behaviour by various kinds of people. Whether the intended behaviours are chilled, or otherwise constrained, is a critical issue: in free and democratic nations, substantial impositions on people need to be justified, and to be seen to be justified. A primary motivation for this analysis is to assess the extent to which the justification exists, is being communicated, and is being subjected to critical assessment. This is particularly important in a country where the actual risks are extremely low- particularly when compared to deaths and injuries on the road system (c. 1,600 p.a.), but even to deaths due by drowning (c. 200 p.a.) and assault (c. 200 p.a.), and possibly deaths due to bee and wasp stings (c. 2 p.a.) and shark attacks (c. 1 p.a.).

The continuing rare incidence of successful terrorist attacks may of course now be framed as either over-investment in anti terrorist measures at a level inappropriate for the risks – or as a 'successful investment'. Claims of 'nil-event success' are easily made, but a naturally sceptical public needs to be convinced.

The paper commences by examining the ways in which surveillance represents an element of security strategy. It then surveys the field of transport surveillance, and examines the social impacts of transport surveillance. The aim throughout is to focus on issues that are relevant to surveillance generally. Conclusions are drawn about the extent to which surveillance, as it has been imposed in the context of 'the war on terrorism' rhetoric, has been publicly justified, and can continue to be imposed as it has been since September 2001.

2 The positive functions of surveillance

This section examines the nature of surveillance as a security tool, and the benefits it can deliver. It first describes the notion of security safeguards, then defines surveillance, outlines the special cases of location and tracking, and places surveillance in the context of security safeguards generally.

2.1 The purposes of security measures

The term ‘security’ is used in at least two contexts: as a condition in which harm does not arise, despite the occurrence of threatening events; and as a set of safeguards designed to achieve that condition. Threats exist, variously natural, accidental and intentional. Threatening events, in which a theoretical threat becomes real, give rise to harm. They do this by impinging on vulnerabilities, which are aspects of a system that render it susceptible to harm arising.

Safeguards or security measures can be devised to address threats, to monitor vulnerabilities, and to ameliorate harm. Security safeguards may be designed to perform one or more of the following functions:

- **deterrence** of unwanted behaviour (e.g. threats of punishment or retaliation);
- **prevention** of unwanted behaviour (e.g. controls on access to materials that can be used to prepare explosives);
- **preemptive interception** of acts **preparatory** to unwanted behaviour (e.g. road-blocks);
- **interception** of acts that themselves constitute unwanted behaviour (e.g. preclusion of vehicle access to particular zones, to prevent them from getting close enough to an intended target to inflict major damage);
- **detection** of instances of unwanted behaviour that have occurred (e.g. monitoring of explosions);
- **investigation** of instances of unwanted behaviour that have occurred (e.g. cordoning off of blast-zones to enable forensic examination);
- **retribution** for instances of unwanted behaviour that have occurred (e.g. prosecution for a criminal offence, vengeance attack, torture, execution);
- **building of public confidence** (e.g. announcements of investment in various safeguards such as port and aircraft security measures). These announcements may or may not have a clear nexus with measures that could have prevented past attacks or reduced their impact.

Any proposed security safeguard needs to be assessed in order to understand what contributions it is capable of making to those functions,

what conditions must exist for the objectives to be achieved, what susceptibility they have to countermeasures, and what new vulnerabilities they give rise to. The identifiable costs and the other (to date almost invariably uncosted) social behaviour, freedom, privacy etc disbenefits of a security safeguard need to be taken into account. These include not only the direct costs, but also the opportunity costs, by which is meant the opportunities that are foregone by committing specific resources to a particular security safeguard rather than to alternative uses.

2.2 Surveillance

The term 'surveillance' derives from the fraught times of the French Revolution at the end of the 18th century. It refers to the systematic investigation or monitoring of the actions or communications of one or more persons. It is useful to distinguish several categories:

- **Personal Surveillance**. This is the investigation or monitoring of an identified person. In general, a specific reason exists for the investigation or monitoring. It may be applied as a means of deterrence against particular actions by the person, or repression of the person's behaviour (e.g. identity cards linked to mass databases accessible by enforcement agencies; and electronic road pricing systems without a true anonymity option – Wigan 1996);
- **Mass Surveillance**. This is the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organization. It may also be used for its deterrent effects (e.g. the claims made about the feasibility of crowd facial recognition systems);
- **Object Surveillance**. This is the investigation or monitoring of an object of some kind, to detect movement or a change of its state (e.g. anti-theft image processing movement detection systems); and
- **Area Surveillance**. This is the investigation or monitoring of physical space, which may or may not include objects or people (e.g. CCTV, pedestrian counting systems, and proposed widespread sensor systems utilising grid computing).

The basic form of surveillance is physical, and comprises watching

(visual surveillance) and listening (aural surveillance). Monitoring may be undertaken remotely in space, with the aid of image- amplification devices like field glasses, infrared binoculars, light amplifiers, and satellite cameras, and sound- amplification devices like directional microphones; and remotely in time, with the aid of image and sound-recording devices. In addition to physical surveillance, several kinds of communications surveillance are practised, including mail covers and telephone interception. The popular term ‘electronic surveillance’ refers to both augmentations to physical surveillance (such as directional microphones and audio bugs) and to aspects of communications surveillance, particularly telephone taps.

Since the explosion in the scale and accessibility of collections of data about things and people, data surveillance has developed as a convenient and relatively inexpensive approach to monitoring. Dataveillance is “the systematic monitoring of people’s actions or communications through the application of information technology” (Clarke 1988, 2003a). It depends on the acquisition of data, preferably streams of data, and preferably from multiple sources.

2.3 Location and tracking

Some surveillance technologies support the location of specific objects or individuals in some space. Further, they may support tracking, which is the plotting of the trail, or sequence of locations, that is followed by an entity within that space, over a period of time. The ‘space’ within which an entity’s location is tracked is generally physical or geographical; but it may be virtual, e.g. a person’s successive interactions with a particular organisation (Clarke 2001).

Due to timeliness limitations, data generated by a surveillance measure may only be able to be used for retrospective analysis of a path that was followed at some time in the past. A ‘real-time’ trace, on the other hand, enables the organisation undertaking the surveillance to know where the entity is at any particular point in time, with a degree of precision that may be as vague as a country, or as precise as a suburb, a building, or a set of co-ordinates accurate to within a few metres.

A person in possession of a real-time trace is in many circumstances able to infer the subject’s immediate future path with some degree of

confidence. Given a certain amount of data about a person's past and present locations, the observer is likely to be able to impute aspects of the person's behaviour and intentions. Given data about multiple people, intersections can be computed, interactions can be inferred, and group behaviour, attitudes and intentions can also be imputed.

Location technologies therefore provide, to parties that have access to the data, the power to make decisions about the entity subject to the surveillance, and hence to exercise control over it. Where the entity is a person, it enables those parties to make determinations, and to take action, for or against that person's interests. These determinations and actions may be based on place(s) where the person is, or place(s) where the person has been, but also on place(s) where the person is not, or has not been. Surveillance technologies that support tracking as well as location extend that power to the succession of places the person has been, and also to the place that they appear to be going.

2.4 Surveillance as a security measure

Surveillance can be utilised as a security safeguard. But it is a safeguard of a specific kind, and it requires careful assessment in order to appreciate what it can and cannot contribute, under what circumstances, and at what costs.

Surveillance is essentially an intelligence activity. It may be designed for any of several purposes:

- to **anticipate** a violation. For example, a package that has been stationery and unattended needs to be checked;
- to **detect** a violation. For example, unusual patterns of activity in a passageway may lead to the inference that violence is occurring. This may also play a role in anticipating further violation, e.g. because the violence may spread, or because the pattern of activity is sometimes associated with attempts to disguise or obfuscate;
- 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.

Generally, a surveillance scheme designed for one of these purposes may not contribute a great deal to others. Security strategies based on anticipation of an action generally do not- and often cannot- work on the

basis of verified or verifiable evidence, but rather on profiling, and on narrowing down the range of groups and individuals who might be planning an action, enabling pre-emptive measures.

The capacity of surveillance to assist with the performance of the various security functions identified in section 2.1 above can be analysed as follows, with a very common traffic enforcement system used to provide immediately recognisable everyday examples:

- **deterrence**. Covert surveillance is unlikely to have much deterrent effect. On the other hand, if surveillance is known, or at least perceived, to be conducted, but the locations are unknown, then there may be a broad chilling effect on behaviour, at least of some categories of individual, or of some categories of behaviour. Overt surveillance may also have deterrent effects, but a considerable set of conditions needs to be satisfied. The relevant individual needs to know, and believe, that surveillance is being undertaken, and needs to consider that it represents a threat to themselves. It is of little value in the cases of crimes of passion, and in circumstances in which the individual is not concerned about being identified and found after the event. It therefore has no value whatsoever in the case of individuals committing suicide attacks. It is also known from various studies that surveillance tends to displace behaviour rather than to prevent it, and hence it is of limited value where vulnerabilities are widespread, or otherwise exist outside the area that is subject to monitoring. For example, the use of dummy red light and speed cameras enhances the deterrent effects of actual visible and working cameras (although it has been shown that they need to be backed by random undisclosed cameras and speed measurement devices);
- **prevention and interception**. Surveillance by itself cannot prevent acts. It may be an element within a conglomerate of measures, which combine to prevent an act being performed. This depends upon the existence and maintenance of the relevant resources, effective linkage between the surveillance measures and the active components, and the ability of the active components to mobilise sufficiently quickly to prevent or intercept the act. For example, the use of widespread automatic number plate recognition depends on police on duty in vehicles to undertake interception;

- **detection**. Surveillance may provide a basis for establishing the fact that an event has occurred. This depends upon effective linkage of the monitoring activities with measures to record the data, and with (probably human) capabilities to appreciate the significance of the data. For example, automatic speed camera photographs may be examined visually after they are collated;
- **investigation**. Surveillance may provide information of assistance to an investigation into an event that has occurred. This depends upon effective linkage of the monitoring activities with measures to record the data, in a form accessible and useful to the investigator. For example, CCTV records on toll roads;
- **retribution**. Surveillance may provide a basis for taking action against the perpetrator of an event, or against the person responsible for the existence of the vulnerability that was impinged upon. This depends upon data quality. In a great many cases, for example, video-surveillance provides data whose evidentiary value is inadequate primary evidence in criminal cases;
- **building of public confidence**. Announcements of the existence of surveillance measures may bolster confidence that something is being done about the likelihood of threats becoming real, and doing harm.

Within this generic framework, the following section considers various forms of surveillance that are applied in the transport context.

3 Transport surveillance

The term transport is used in this paper to refer to all forms of conveyance, whether intended for freight or for individuals, and irrespective of the mode, hence including road, rail, water and air transport. This section provides a brief survey of surveillance in transport as a whole, supplemented by mini-cases that provide insight into patterns of use, and impacts and implications.

3.1 The nature of transport surveillance

Transport surveillance may be focussed on an area, such as a container loading-point, or an inter-modal interchange. Alternatively, it

may be oriented towards objects, including installations such as a gate, vehicles, and items of cargo. Applications include video-recording, spatial logging of vehicle location and movement, and bar code and RFID usage in supply chains. Surveillance may be focussed on individuals, either directly, or by inference, based on their association with one or more areas, one or more objects, or both.

Transport offers both real-time and retrospective surveillance opportunities. Some real-time contexts also provide the capacity to pick out vehicles of interest, to retrospectively trace their connections with other vehicles and other locations, and to thereby infer their associations and patterns of behaviour. Some surveillance measures provide the capability to predict with a degree of confidence the likely destination of a vehicle or person, and even to impute the person's intentions.

Surveillance designs that are concerned primarily with people include:

• in public transport:
- transport smart cards that deny an anonymous option;
- electronic tolling schemes that deny an anonymous option;
- electronic passports;
- service-denial blacklists such as 'no fly' lists (to date not apparent in Australia at least, although there have been some instances of judicially-imposed denial of access to places such as sporting venues);

• in self-driven vehicles:
- spatial logging of vehicles, and inference of the duration of movement and the location and timing of stops;
- chip-enhanced drivers' licences capable of carrying, and disclosing, additional data;
- automatic number plate recognition (ANPR) schemes;
- medical alert systems linked to vehicles;
- driver monitoring via engine management chips;
- time use surveys of individuals using GPS technologies;

• as consumers:
- RFID usage in supply chains extended to product-purchaser monitoring;

• as workers involved with freight movement:
- positive vetting;

- location and activity monitoring.

Such elements of transport-related surveillance create the scope for enormously detailed and precise surveillance of individuals' movements, activities, and personal and business linkages. The privacy impacts of these measures are potentially quite extreme, because they create intensive trails which create the scope for location and tracking, and hence they create the scope for many additional applications for many more purposes.

Surveillance to assist with security has long been a major issue in goods transport, as loads may be very valuable, and loads may be dangerous. The monitoring of freight transport vehicles has long been accepted as appropriate, and the side-effect of driver surveillance has been worked through over quite some time, starting with automatic vehicle logging systems, in order to achieve an acceptable balance (Wigan 1996).

But surveillance is now being extended to encompass the great many individuals associated with transport of loads into and out of ports and interchange facilities. This draws into the surveillance net people who are far removed from the driving task. Whereas the monitoring of road transport drivers and train drivers was the subject of prior consultative processes and negotiated and balanced features, these extensions have not had the benefit of such interactions.

3.2 Mini-case: speed management

Speed management strategies can be developed in several different ways. For example, the use of covert cameras has been shown to be effective in securing generally lower traffic speeds, and to be more effective than the use of cameras whose locations are publicly declared. Overt cameras, on the other hand, act as a warning-marker for high-risk locations. The use of covert cameras, especially in what are apparently safe areas and locations, has the effect of reducing public trust in the reasonableness of the speed management strategy. This must be balanced against the general effect of reduction of the speed environment as a whole.

This tension has much in common with surveillance and security

strategies, where the pin-pointing of the covert surveillance can undermine the deterrent effect of the strategy, whereas if it is not disclosed at all then the general impact will be lower than if it is intensively focussed on specific locations or systems. This tension between community trust and general effectiveness and deterrence needs to be finely balanced, as indeed is evident in the continuing public debates about speed camera strategies, which oscillate between visible deterrence and systems-wide general impact targets. The system-wide effects of covert enforcement are significant in terms of behavioural modification, but one price of this strategy is a greater distance between the police and the community.

Distinctions need to be drawn between different groups involved in transport. Those employed in transport appreciate that some controls need to be imposed, whereas for the general public a quite different set of standards applies. For example, a Fleet Management system that can launch alerts when a truck-driver is speeding is perceived very differently to the same system applied to every vehicle in the private fleet. Such contextual changes can make a very big difference. Enforcement and intelligence bodies may not always appreciate this.

There are similarities between the security strategies of direct after-the-event prosecutions and pre-event actions based on probabilities and the speed strategies. The speed strategies of direct, credible and immediate on-the-spot enforcement strategies and their clear nexus with civil law, evidence and intent and the system-wide covert automated penalty approach which leaves many weeks between event and reinforcement are both still capable of civil demonstration and evidence, while pre-emptive security actions are not, and cannot be.

In short, the medium-term effectiveness of surveillance schemes is dependent upon social acceptance and trust (Daniel et al. 1990, Wigan 1995).

3.3 Mini-case: automatic number plate recognition

One automated enforcement system that is attracting much attention at present is Automatic Number Plate Recognition (ANPR). This involves a camera stationed near a road, capturing images of the numberplates of passing vehicles, using pattern-matching recognition- in a manner similar

to Optical Character Recognition (OCR) for documents- and making the data available to back-end applications.

ANPR data can be used to automatically generate and despatch notices of speed violations, and to charge vehicle-owners for road-usage. ANPR can also be used to compare passing registration-numbers against a 'blacklist', reflecting, 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 past by a person who is the subject of personal surveillance. This capacity is already in use in the U.K. where ANPR has been touted as "[future] infrastructure across the country to stop displacement of crime from area to area and to allow a comprehensive picture of vehicle movements to be captured" (Connor 2005). It has been floated by at least two State Governments in Australia.

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. These schemes have been introduced with little or no public involvement, little or no discussion in parliaments, and without any apparent controls over use, abuse, data retention and function creep.

3.4 Mini-case: the chip-based passport

A passport was originally a document, provided by a sovereign to an individual, which requested officials at borders and in seaports to permit the bearer to enter. The notion was known to English law at least as early as 1300. At the end of the nineteenth century, passports were issued on request, by the governments of various countries, in order to provide evidence of nationality, and, by implication, of identity. But there were few circumstances in which it was actually necessary to have one, even when crossing national borders. After World War I, in a climate of mass movements of displaced persons, it became increasingly common for governments to demand documents which evidenced a person's nationality. An international conference in 1920 established the present passport system. During the inter-war period, the passport became a near-universal requirement for international travel. It has remained so (Clarke 1994, p. 16).

Government agencies have grasped the opportunity presented by the post-September 2001 terrorism 'managed hysteria' to arrange parliamentary approval for a new form of passport that embodies various technologies. In Australia, the Passports Office actively avoided making information available to the public, and indeed to the Parliament. Even after the new scheme was launched in October 2005, the information made available remains so scant as to be almost worthless from the viewpoint of someone trying to understand the scheme's features (DFAT 2005).

It appears that the document includes a contactless RFID 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. The original proposals were subject to enormous vulnerabilities of a privacy nature, extending to the point of facilitating identity theft.

The protections ultimately implemented are claimed to be compliant with a specification approved by an international association of governments (ICAO 2004). If effective, then the worst of the data-leakage problems in the original proposals have been overcome. But it remains unclear what additional data the chip contains now, what it may contain in the future, and who will be permitted the capacity to access the data.

Among the powers that the Department achieved by submitting a replacement statute for brisk and almost entirely unconsidered approval by acquiescent law-makers was the freedom to implement biometrics, in whatever manner the Department saw fit, subject only to convincing their own Minister. This was done in such a manner as to avoid even mentioning the word or concept of biometrics in s.47 of the re-written Passports Act. This represents an extraordinary delegation of power to public servants.

The mythology used to produce time-pressure for the provision in the Bill was that a chip-based scheme carrying a biometric was necessary to retain Australian status under the U.S. visa-waiver program for short-term visits. This was simply presumed to be extremely important. It is unclear how significant the claimed justification is, even for the small minority of Australians who do business in the U.S. or travel there as tourists, and it appears never to have been subjected to analysis or public consultation.

DFAT (2005) states that “facial recognition technology is being introduced to coincide with the release of the ePassport”. On the other hand, the accompanying press release of 25 October 2005 said circumspectly that the new passport “will enable the implementation of cutting-edge facial recognition technology”; so it is unclear from the available documentation whether or not the Department has yet implemented it.

Facial recognition technology has been trialled in the SmartGate scheme run by the Australian Customs Service (ACS). In responding to criticisms of the technology’s effectiveness (e.g. Clarke 2003b), ACS has acknowledged that it is not a security feature, but rather a ‘customer service’ feature. The very probable failure of the facial recognition technology appears likely to be used 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.

These new forms represent a potentially enormous 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 in circumstances other than at national borders. The ability of an 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.

3.5 Data linkage

The examples outlined above need to be seen in the context of widespread endeavours to pool personal data sourced from different programs. The tracking of identified individuals generates increasingly intensive data-sets. The existence of data about movement paths creates risks in relation to dangerous cargo, valuable cargo, and persons of interest. Further, through correlation of locations and times in entries for one person with the entries for another person, social networks can be inferred, at least with probabilistic confidence.

The many transport surveillance applications produce multiple

data-trails. Linkages and correlations across depot, toll-road, ANPR and public transport schemes, for example, are capable of generating yet more detail about a person's movements and habits. Such intrusiveness is a matter of sensitivity to corporate strategists, deal-makers and salesmen as much as it is to individuals in less exalted occupations. Those who have in mind to exercise rights of political speech and action are increasingly likely to be confronted by this data, directly from national security and law enforcement agencies, or more likely via their employers, Centrelink, and grants administrators.

Collections of tracking data are capable of being linked with data from other sources, variously for personal data surveillance (of a suspect), or for mass data surveillance (in order to generate suspects). Data may be acquired from many sources, such as consumer marketing databases, government registers, and health systems. The operators of each system, is similarly tempted to seek additional sources to link with their own, and barter is an attractively low-cost approach. Data protection laws are already very weak, and are easily subverted and amended. They represent only a limited barrier for powerful corporations and government agencies.

The explosion in surveillance opportunities needs to be seen in the light of strenuous efforts to destroy the longstanding norm of anonymity in both travel, and the conduct of large-volume / low-value transactions. In the space of a decade, public transport tickets and toll-road payments have been changed to preclude cheap and convenient travel in the absence of an authenticated identifier- simply through refusal to accept payment other than by credit-card and debit-card. Such cards are subject to 100-point checks as a result of function creep applied to measures that were implemented ostensibly to enable the monitoring of money-laundering. Those schemes have been in place for years, with barely any significant results. The solution has of course not been to admit that they do not work, but rather to claim that they will, provided that they are extended yet further.

The public has enjoyed anonymity in many transactions, and the freedom to use multiple identities. Some uses are for criminal or anti-social purposes, but the vast majority are harmless to society and important to individuals. Examples of people for whom multiple identities

are a matter of sheer physical safety include undercover national security and law enforcement personnel, protected witnesses, psychologists and counsellors and many other groups who need to maintain separation between their private and professional personas - and obscuration of their locations.

Transport-based security systems targeting people, whether directly or only incidentally, are capable of rapidly breaking down longstanding protections. It is remarkable that schemes could have been introduced so precipitously, and without a debate as to how society handles these important issues.

4 Social impacts of transport surveillance

The examples of transport surveillance outlined in the previous section evidence a wide range of serious social impacts and implications. They have not yet been subjected to a coherent evaluation of their privacy impacts. Nor have the broader social effects of such systems yet been thought through.

A study of surveillance in other settings would appear very likely to generate a long list of comparable problems. For example, some access control systems to premises and to computer-based systems are being linked to criminal records (in such areas as registration of teachers and child-care workers), and to health records (e.g. for pilots and train-drivers). Such inter-system data linkages open up high probabilities of misuse, and of automated errors arising from conflicts and ambiguities in identity-matching, and in data definition, accuracy, precision and timeliness. They therefore give rise to many forms of socially expensive stress.

Consideration of these schemes leads to a number of inferences about their design features:

- there is a widespread lack of appreciation of the distinctions between law enforcement and national security activities, despite the fact that they have fundamentally different philosophies, justifications and processes. Law enforcement is aimed at accurate identification of an offender, presentation in court of evidence of that person’s guilt, withstanding the person’s legal defences, and securing conviction.

National security, on the other hand, is largely anticipatory, is based on suspicion at least as much as evidence, and is seldom able to be defended against. These philosophies collide in any integration process, giving rise to social issues and economic costs;

- there is insufficient understanding that the 'chilling' of behaviour that is perceived to be 'deviant' creates the risk that the behaviour of other people will be modified as well, in ways that are harmful to individuals, and to society. Innovation and progress in all walks of life are fundamentally dependent on behaviour that is (initially) perceived to be 'deviant';
- there is an implicit presumption by policy-makers and designers that individuals are to be forced to use just one identity. This is despite the widespread usage and long history of, and common law support for, multiple identities. Existing law recognises only offences that involve the abuse of multiple identities, e.g. to enable fraud. The safety of psychologists, for example, particularly in highly-charged areas such as the family court, is dependent on the avoidance of discoverable links between their professional and private identities and addresses;
- there is a further implicit presumption by policy-makers and designers that individuals are to be denied anonymity, and even denied strong forms of pseudonymity (Clarke 1999). They thereby become exposed to authority, and to every other organisation that can negotiate or otherwise gain overt or covert access to the relevant data;
- surveillance schemes are being developed without any guiding philosophy that balances human rights against security concerns, and without standards or guidance in relation to social impact assessment, and privacy design features.

In addition, control issues emerge:

- there are very limited constraints on abuses of surveillance systems (in such forms as independent oversight, audit, investigative resources and activities, criminal sanctions and enforcement). There has always been a shortfall in controls of these kinds, but the freedoms granted to national security and even law enforcement agencies in enactments passed during the last several years by parliamentarians 'asleep at the wheel' far exceeds previous levels of

laxity;

- there are very limited constraints on the linkage and consolidation of data-holdings and identities, and the associated destruction of protective ‘data silos’ and ‘identity silos’;
- there are very limited constraints on ‘function creep’;
- there are very limited constraints on the data-mining of organisations’ own holdings and of consolidated databases. This is despite the enormous risks involved in drawing inferences from highly heterogeneous data drawn in highly varied ways from highly diverse sources, each of which was designed for narrow, specific purposes;
- there is a desperate shortage of credible audits of the performance of surveillance schemes, and of their compliance with such control mechanisms as exist. Privacy Commissioners and other nominal regulators, when starved of funding, commonly treat their audit programs as the first sacrifice.

There are clear antidotes to these ills. Techniques for the evaluation of proposals for technology applications are well-established, in such forms as cost-benefit analysis and the more appropriate cost-benefit-risk analysis (Clarke & Stevens 1997). The stakeholder concept is well-known to encompass not just government agencies, technology providers, and business ‘partners’, but also affected individuals. The process of privacy impact assessment (PIA) is well-established (see Clarke 1998). Focus-group techniques are available. Representative and advocacy organisations are available to consult with, and the principles that guide effective community information and consultation processes are well-known. Agencies have no excuses for failing to inform and failing to consult. But some, such as the Attorney General’s Department, often prefer to ignore public opinion, and exercise their power.

What is lacking is not the ability to specify appropriate processes, but rather courage on the part of parliamentarians to ask hard questions, and to say ‘no’ to the national security community. It could be argued that courage is also lacking on the part of senior executives, who are failing to oppose excessive demands from national security and law enforcement agencies. Those senior executives are compromised, however, and unlikely to take actions to benefit freedoms.

Social control is a primary motivation for many senior government executives. Carriage of the original Australia Card proposition was after all with Health, supported by Treasury and to some extent Social Security and Immigration (Clarke 1987). The mandarin class appears to subscribe to the belief that there will be a 'trickle-down effect' from the recent spate of authoritarian initiatives, which will benefit mainstream agencies.

5 Conclusions

Transport security systems eat into the social space, and they have been doing so in an unaccountable manner. It is far from clear that the ostensible reasons for their introduction are justified, and the already well-established practice of function creep is steadily eroding the credibility of Government claims for various forms of new cards. Their extended application would be even more intrusive and threatening.

Proposals for new and enhanced surveillance schemes, in transport as elsewhere, must be measured against the norms of security analysis and design. It is clear that the dependence on rushed presentation of proposals to Ministers and the Parliament under the guise of 'measures necessary in order to conduct the war on terrorism' have been a smokescreen for the absence of any such assessments having been undertaken even behind the closed doors of national security agencies.

The agencies that are imbued with the surveillance and intelligence culture are utilising their opportunity to the utmost, and can be expected to extend the window as long as they can. They have little interest in ceding the ground they have won through the fog of misinformation. What community leaders must now do is appreciate the massive harm that surveillance measures are doing to public confidence in its institutions.

It is increasingly obvious to the public that not only are there few wolves to cry out about, but the impediments that have been built are impediments to normal activities of normal people, not to the violent activities of such terrorists and latent terrorists as exist in this country.

The lack of legitimacy will rapidly undermine the preparedness of the public to accept substantial constraints that are available for government control of miscreants rather than for the claimed terrorist threat. Recourse to the excuse of 'drug barons' and 'organised crime' is on similarly fragile

ground because of the ongoing failure of data surveillance in particular to enable them to be brought to book. The collapse in public confidence will accelerate as abuses come to attention, and as the reality of the various schemes' privacy-threatening features and lack of controls hits home.

Community trust in the State cannot be sustained in the absence of transparency. Individuals and communities are being precluded from contesting claims made by the State of the necessity of extremist measures. The lessons of the speed campaigns of the last 20 years makes it all too clear that this is a pivotal point, as community social capital is inevitably undermined by intelligence-based pre-emptive actions.

Cooperation by the public, and by the workers whose job it is to operate and maintain such schemes, can be withdrawn at short notice if trust is not established and maintained. The integrity of surveillance schemes, in transport and elsewhere, is highly fragile.

The last few years have seen a headlong rush to secure national infrastructure, and to protect people's physical safety from major acts of violence. This movement embodies major risks to society. The right of freedom of anonymous movement within the country has been suddenly and substantially compromised. The freedoms to be, to think, and in most circumstances to act differently from other people, and privacy and civil rights more generally, are being destroyed, not by terrorists, but by 'friendly fire'.

It is vital that Australians energetically resist not only religious fundamentalism but also national security fundamentalism. Transport is a key area where this could all too easily occur.

References

Note: URLs accessed April 2006.

Clarke R. (1987) 'Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme' Prometheus 5,1 (June 1987), at http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html

Clarke R. (1988) 'Information Technology and Dataveillance' Comm. ACM 31,5 (May 1988). Re-published in C. Dunlop and R. Kling (Eds.),

'Controversies in Computing', Academic Press, 1991, at http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

Clarke R. (1994) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues', Information Technology & People 7,4 (December 1994) 6-37, at http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Clarke R. (1998) 'Privacy Impact Assessment Guidelines', Xamax Consultancy Pty Ltd, February 1998, at http://www.xamax.com.au/DV/PIA.html

Clarke R. (1999) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' Proc. User Identification & Privacy Protection Conference, Stockholm, 14-15 June 1999, at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

Clarke R. (2000) 'How to Ensure That Privacy Concerns Don't Undermine e-Transport Investments' Proc. AIC e-Transport Conf., Melbourne, 27-28 July 2000, at http://www.anu.edu.au/people/Roger.Clarke /EC/eTP.html

Clarke R. (2001) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Infor. Techno. & People 14, 2 (Summer 2001) 206-231, at http://www.anu.edu.au/people/Roger. Clarke/DV/PLT.html

Clarke R. (2003a) 'Dataveillance - 15 Years On' Proc. Privacy Issues Forum, New Zealand Privacy Commissioner, Wellington, 28 March 2003, at http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html

Clarke R. (2003b) 'SmartGate: A Face Recognition Trial at Sydney Airport' Xamax Consultancy Pty Ltd, August 2003, at http://www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html

Clarke R. & Stevens K. (1997) 'Evaluation Or Justification? The Application Of Cost/Benefit Analysis To Computer Matching Schemes' Proc. Euro. Conf. in Infor. Syst. (ECIS'97), Cork, Ireland, 19-21 June 1997, at http://www.anu.edu.au/people/Roger.Clarke/SOS/ECIS97.html

Connor S. (2005) 'Britain will be first country to monitor every car journey' The Independent, 22 December 2005, at http://news.independent.co.uk/uk/transport/article334686.ece

Daniel M., Webber M.J. & Wigan M.R. (1990) 'Social impacts of new technologies for traffic management' Australian Road Research Board, Research Report ARR 184, 1990

DFAT (2005) 'The Australian ePassport', Department of Foreign Affairs, undated but apparently of October 2005, at http://www.dfat.gov.au/dept/passports/

ICAO (2004) 'Biometrics deployment of Machine Readable Travel Documents: Annex I - Use of Contactless Integrated Circuits', International Civil Aviation Organisation, May 2004, at http://www.icao.int/mrtd/Home/Index.cfm

Kopytoff V. (2006) 'Wi-Fi plan stirs big brother concerns Log-on rule would allow Google to track uses whereabouts in S.F.' San Francisco Chronicle, 8 April 2006, at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/04/08/BUGROI5S5J1.DTL

Pollack P. (2005) 'Concerns arise over Google user tracking in SF' Ars Technica, 10 April 2006, at http://arstechnica.com/news.ars/post/20060410-6570.html

Wigan M.R. (1995) 'The realizability of the potential benefits of intelligent vehicle-highway systems: the influence of public acceptance' Infor. Techno. & People, 7, 4 (1995) 48-62

Wigan M.R. (1996) 'Problems of success: Privacy, property, and transactions' In Branscomb L. & Keller J. (Eds.) 'Converging Infrastructures: Intelligent Transportation and the NII', MIT Press, 1996

3

Identity management: is an identity card the solution for Australia?

Margaret Jackson and Julian Ligertwood[1]

School of Accounting and Law, RMIT University

Abstract

The paper explores how an identity card scheme might work in Australia by using the UK Identity Card Scheme as a model. It explores the proposal for a national UK identity card scheme and assesses how it would reduce identity theft and fraud, improve national security, and maintain adequate privacy protection. The paper discusses the legal and social difficulties associated with the introduction of such a national identity card scheme and the issues which arise when a government seeks to broaden the scope of the scheme from identity fraud and security issues to include the efficient and effective delivery of public services. It suggests alternative approaches to ensuring identity management which are consistent with privacy and data protection restraints. This paper should contribute to the development of Federal Government policy in the area of a regulatory and legal framework for identity management.

Keywords: identity card, identity fraud, privacy

[1] The authors wish to acknowledge the support of the Smart Internet Technology Co-operative Research Centre in the development of this paper.

1 Introduction

Arising from its present stated concerns about security, government services fraud, money laundering and a need for an improved way to verify identity, the Federal Government has introduced greater security measures within passports and has proposed placing greater responsibility for verification of identity on some parts of the private sector through the introduction of stricter anti-money-laundering laws (Federal Attorney-General's Department 2005). It has also once again considered the need for a national identity card as part of a broader national identity security scheme.

A number of different proposals to strengthen identity verification have been raised by the Government over the last year or so but the most contentious proposals have been for a new national identity card and for a government services smartcard to replace the existing Medicare card and other benefit cards (Grattan 2006, Riley 2005).

This paper briefly examines the history of identity cards in Australia and discusses the current proposals of the Government to introduce some form of identity card. It examines the recently enacted *Identity Cards Act 2006* in the United Kingdom and explores some of the concerns about that proposal. Finally, it analyses whether or not an identity card scheme would address the Government's concerns about protecting security in addition to the private sector concerns about identity fraud and theft.

2 The Australian Government proposals

2.1 The Australia Card

Australia has a history of registration, personal identification and data collection within both the public and private sectors. The idea of a national identity card is not new. During WWII, Australians were registered under the *National Security Act 1939* (Cth) and *National Registration Act 1939* (Cth) and were given a basic identity card under the 1947 National Security (Manpower) Regulations. The imposition of rations was an incentive for registration and production of the card (Caslon 2005).

It was not for another thirty years, however, before three government

reports published in 1975 suggested that government efficiency could be improved and fraud better detected through the introduction of an identity card system (Jordan 2006). The then Fraser Government took no action about these recommendations at that time. In 1986, the Hawke Government tried to introduce a national identity card, the Australia Card, but there was substantial public opposition to it and, by 1987, 90 per cent of Australians were opposed to the card (Davies 2004). However, the accompanying *Privacy Bill 1988 (Cth)*, which contained Information Privacy Principles about how personal information was to be collected by federal government agencies, was enacted and enhancements to the Tax File Number (TFN) scheme administered by the ATO were enacted with the objective of increasing the Government's capacity to link the identification of specific taxpayers with specific taxable income (Clarke 1987).

2.2 Current proposals

The next attempt to introduce a national identity card in Australia apparently began as a result of the London bombings on 7 July 2005. On 14 July 2005, Queensland Premier Peter Beattie commented on the issue on ABC radio arguing that such a card would be in the interests of national security. When asked about Beattie's comments, Prime Minister Howard did not support them but his own comments were vague and he was reported in the press as not ruling it out altogether in the Government's review of security arrangements (Humphries and Todd 2005). Howard then became more supportive of the idea of an identity card and the Attorney-General subsequently stated that the Government would be examining the possibility of an identity card (Howden, Crawshaw, and Tasker 2005; Australian Privacy Foundation 2005). However, many government ministers were strongly opposed to the idea as the Attorney General himself had been in October 2003 (Baker 2006).

In January 2006, Attorney-General Philip Ruddock announced he was establishing a formal enquiry into whether Australia needed an identity card and how much it would cost to implement it (Priest 2006). He provided no specific information about the purpose of such a card so that it was not clear if the primary focus would be on security, identity fraud, anti-money-laundering or effective government services. However, in an

abrupt turnaround, the Prime Minister and the Attorney-General announced in April that the Government would not be introducing a national identity card but would instead introduce a health and welfare services smartcard (Gratten 2006; Crawshaw 2006).

The proposal for a human services smartcard was discussed at a Cabinet meeting on 26 April 2006. The major purpose of the smartcard, to be phased in from 2008, is to prevent welfare fraud. The card will replace 17 existing benefits cards and will contain a digital photo, a number and signature. A microchip will include a photo, address, date of birth and details of dependants. Emergency contacts and medical information is optional. The cost of setting up the smartcard is about $1 billion over 4 years (Grattan 2006). The smartcard was first raised as a possibility by Minister Hockey during 2005 and, while its main purpose is to reduce welfare fraud, Minister Hockey and his colleagues have also mentioned other uses such as disaster relief payments, medicare refunds and in slashing red tape (Schubert 2005; Bajkowski 2005).

The Government, as part of its National ID Security Strategy and e – Authentication Framework, has also introduced an e-passport with a machine readable microchip that can electronically store biometric and other personal information. The e passport has had its fair share of criticism from privacy groups (Lebihan 2006a) as well as some technical problems with the RFID technology (Lebihan 2006b) but is now being implemented. The Government is also planning to introduce an E – Health medical records system, an eCitizen scheme requiring new citizens to have biometric identifiers (Lebihan 2006c) as well as centralized internet accounts with the Government (Bajkowski 2006).

3 The United Kingdom identity card proposal

3.1 Background

Britain abandoned its wartime identity papers 50 years ago and has not since had a national identity card system, although at least nine of the 25 European Union (EU) members have some form of identity card (London School of Economics 2005). The national identity card has been an unfulfilled pet project of both Labour and Conservative governments in

the UK for more than 20 years.

In April 2004, a draft Identity Cards Bill was published, proposing the introduction of a UK identity card scheme coupled with a national database. Most of the detail was left to future unspecified regulations. There was sufficient opposition to the Bill to ensure that it ran out of time in the run up to the General Election on 5 May 2005 (*Out-Law News* 2005b).

The draft Identity Cards Bill was reintroduced into Parliament on 17 May 2005 and the Government narrowly won a second reading of it in the House of Commons on 28 June, after the Home Secretary agreed to cap the cost to individuals of obtaining the card. There was opposition to the Bill from within the Labour Party, the Tories and the Nationals (*Out-Law News* 2005a). The Bill passed through committee stage and onto the House of Lords. The all-party House of Lords Constitution Committee expressed concerns about the lack of an appropriate separation and limitation of powers, particularly as the Bill proposed that the Secretary of State be responsible for the scheme, rather than a new entity, responsible to and reporting to parliament (House of Lords Select Committee 2005).

On 16 January 2006, the House of Lords advised the Government that it would not approve the Identity Cards Bill without full details of the costs for the scheme (*Out-Law News* 2006). However, once satisfied about the costs, the bill was finally passed by the House of Lords and it became law on 30 March 2006.

3.2 The Act

The *Identity Cards Act 2006* (UK) empowers the Secretary of State to establish a National Identity Register. The purposes of the Register are stated in s 1(3):

> … to facilitate, by the maintenance of a secure and reliable record of registrable facts about individuals in the United Kingdom –
>
> (a) the provision of a convenient method for such individuals to prove registrable facts about themselves to others; and
>
> (b) the provision of a secure and reliable method for registrable facts about such individuals to be ascertained or verified wherever that is necessary in the public interest.

Something is in the public interest if it is in the interests of national security; or is required for the purposes of the prevention or detection of crime, of enforcement of immigration controls, of the enforcement on prohibitions on unauthorised working or employment, or for securing the efficient and effective provision of public service (*Identity Cards Act 2006* (UK) s1(4)).

Sections 3, 6 and 7 and Schedule 1 describe the information about an individual, generally all people residing in the UK over 16 years of age, that will be collected and retained in the Register:

- Full names and other known names
- Date and place of birth (and date of death)
- Gender
- Physical characteristics
- Biometric information (which could include signatures, facial recognition, digital photos, iris scans or fingerprints)
- Every residential address with dates
- Nationality
- National Identity Registration number, identity card number, National insurance number, passport number, driver's licence, work permits, immigration documents as well as other reference numbers allocated
- Validation information – including information provided to support initial registration or a modification to it
- 'Steps taken' by the authorities to identify an individual or verify information provided to the Register
- Security information, such as a PIN number, password or code, for the purpose of providing information to the register.
- Information about occasions on which information recorded about an individual in the Register has been provided to any person.

There is no time limit on how long the personal information can be kept on the Register. It may be retained 'for so long as it is consistent with the statutory purposes for which it is recorded' (s3(1)). There also does not appear to be a right of access to the information stored about them on the Register by the individual. The Act requires an individual to update information about themselves already provided (s10(1)) but only the Secretary of State has the power to correct information if he or she judges it to be appropriate (s3(6). The Secretary will have the power to obtain

information about an individual without their consent from third parties (s19(2)) and will be able to grant access by a range of public authorities in the public interest to individual's personal data (ss17-20). Access will not be subject to the consent of the individual in these instances.

The Act empowers the Secretary of State to enforce registration (s7). It also establishes new offences for the possession of false identity documents (s25), setting out civil and criminal penalties (ss25 and 31). It will not be compulsory to carry a card (s13(3)) and, with the exception for the provision of public services or where a person is given the option of using reasonable alternative methods of establishing their identity (s13), it will be unlawful to require an individual to produce an identity card (s16).

The UK scheme centres around the creation of a National Register which will be able to be accessed by over 265 government departments and, if the individual consents, by about 44,000 private sector organisations (London School of Economics 2006). How private sector organisations will be able to obtain permission to access the Register is not clear as the Government responses to queries about how the process might work have been contradictory and unclear (London School of Economics 2006). These organisations will be required to be validated to access the Register and will require appropriate scanning and other technology to access the Register and to read the card. There will be a transaction fee for each identity check, which will presumably be passed onto the individual concerned.

The UK Government argues that an identity card scheme will help to tackle crime that relies on the use of false identities, such as terrorism, drug trafficking, money laundering, fraud through identity theft, illegal employment and immigration. It also argues that the Identity Card will enable people to access current services more easily, provide a watertight proof of identity for use in everyday transactions and travel, and provide a means of providing more efficient services.

However, two authoritative negative responses to the Identity Card Bill (as it was at the time) came from the Information Commissioner (UK) and the London School of Economics (LSE). The major concern of the Information Commissioner is that the information collected by the Government may not be fair and proportionate to the public interest purposes of collecting personal information (Information Commissioner

2005).

The Information Commissioner argued that the measures in relation to the National Identity Register and the data trail of identity checks on individuals risk an unnecessary and disproportionate intrusion into individuals' privacy (Information Commissioner 2005). The measures are not easily reconciled with fundamental data protection safeguards such as fair processing, deleting unnecessary personal information and the right of individuals to access and correct data stored about them. An effective identity card could be established avoiding these unwarranted consequences for individuals. In his view, the primary aim of the Government with this legislation should be to establish a scheme which allows people to reliably identify themselves rather than one which enhances its ability to identify and record what its citizens do in their lives (Information Commissioner 2005).

The Commissioner also indicated a number of aspects of the proposals in the Bill that were potentially inconsistent with the requirements of the Data Protection Principles as set out in the *Data Protection Act (UK) 1998* including that the breadth of the five purposes specified in the Bill could lead to function creep in unacceptable areas of private life, that the technical and administrative arrangements proposed in the Bill lack independent oversight, and that the use of secondary legislation and regulations will allow the expansion of identity checks via other legislation and the ability to check the Register even though no card has been issued (*Out-Law News* 2004a, 2004b).

The LSE undertook a major investigation into the Identity Cards Bill, producing a report titled *The Identity Project: an assessment of the UK Identity Cards Bill and its implications* on 27 June 2005. It stated that the proposals were too complex, technically unsafe, overly prescriptive and lacked a foundation of public trust and confidence. The Report concluded that the proposal would be very expensive and that it would alter the nature of British society.

The LSE Report estimated the likely cost of the ten-year rollout of the scheme to be between £10.6 billion and £19.2 billion. These estimates were considerably higher than the government estimates of £5.8 billion (*eGov Monitor Weekly* 2005) and provided the basis for the rejection of the Identity Cards Bill in the House of Lords on 16 January 2006.

4 Will identity cards satisfy the concerns of governments?

The UK Government has not been able to show clearly how its Identity Card and Register will be used to reduce terrorism and other security threats, although this is part of the stated purpose for their introduction. For instance, alleged terrorists in the United States, the UK, Spain and Australia have not lacked identity papers (Caslon Analytics 2005). It is the intent of terrorists which is unclear, not their identity.

Further, the LSE Report examined government statistics from 2002 on the cost of identity fraud and concluded that the card would have no or very minor impact on identity related VAT fraud, money-laundering (as identified by Customs and Excise), health services fraud, immigration fraud, insurance fraud, credit card fraud, and identity theft fraud (London School of Economics 2005). The only category of identity fraud in which an identity card could be used effectively was that of identity related social benefit fraud, estimated to be approximately £35 million per annum (or 1% of total benefit fraud) (London School of Economics 2005). There is also a possible use in stopping temporary workers from outstaying their entry visas. So if identity card schemes such as that proposed in the UK have limited effectiveness, it would appear important to restrict their implementation to those individuals who are involved, such as those on welfare.

In relation to concerns about privacy, the Australian Privacy Principles are at least as strong as the UK Data Protection Principles and therefore if the proposals in the UK Act are potentially inconsistent with the UK Data Protection Principles, then a similar Act in Australia would certainly be inconsistent with both the Information Privacy Principles set out in the *Privacy Act 1988* (Cth) which apply to federal government agencies and the National Privacy Principles which apply to the private sector.

The general concerns expressed in relation to the UK Act by the Information Commissioner are also valid in the Australian context. The Commissioner argues that the measures in relation to the National Identity Register and identity card may become an unnecessary and disproportionate intrusion into an individual's privacy.

Data protection principles are based on the premise that only personal information needed for a specific and defined purpose will be collected by organisations, and that it will be retained for a limited time, then destroyed

once the purpose has been fulfilled (Jackson 2001). Access to personal information by third parties is restricted and individuals should be notified of likely recipients at the time of collection. A key aspect of all data protection principles is that the individual will have access to what is stored about them and will be able to amend incorrect data (Jackson 2001). The UK scheme provides few of these obligations, allowing collection of data for fairly ill-defined purposes, access to the data by a broad range of third parties, no limits on retention, and no right of access by individuals.

Identity cards *per se* are not 'bad'. Australians are used to different forms of identity cards already. Australians who wish to travel overseas accept that they must have a passport. Our driver's licence and our current Medicare Card are perceived as being quite acceptable as they have clearly defined purposes. The former is now being used as a form of identity card, for example, when collecting electronic tickets at airports or when seeking to pay for goods by cheque. It is the photo on the licence which is the key to its use, rather than the number itself. On the other hand, it is the number on the Medicare Card which is important.

It is the multifunctional nature of the identity card as seen in the UK proposal which causes alarm. The entire adult population does not need a card for the Government to stop welfare fraud; only those receiving welfare payments. Similarly, it is excessive to require a national identity card to tackle immigration fraud. A national identity card may be appropriate for addressing terrorism but the government needs to show how that card will work to achieve this purpose.

The Australian Government is already developing a government verification service to allow for the verification of documents used for identification, such as a birth certificate, and is addressing health and welfare fraud through the human services smart card initiative. These initiatives appear to be a sensible approach to specific problems. They are attempting to address one specific problem with a specific solution.

However, there has been no publicly available document released about the human services smartcard. The only information about the proposal has been through Government press releases and private press briefings. Since the smartcard was first raised by Minister Hockey in early 2005, the government's stated objectives for it have expanded well

beyond the original purpose of reducing welfare fraud. It is difficult at this stage to comment on whether the Government is proposing to use it as a defacto national identity card. Certainly, it has potential to be developed as one.

5 Conclusion

The main question arising from any proposal to introduce an identity card is whether its negative impact on the human and legal rights of citizens is sufficiently balanced by the benefits arising from the reduction of the problems it is designed to reduce, such as identity fraud or threats to national security. There are, of course, many other questions relating to the feasibility of the technology proposed and the cost of the scheme but these are beyond the scope of this paper.

The Australia Government appears to have deferred consideration of an identity card scheme similar to that introduced in the UK which is probably wise, given the criticisms of the UK model and the Australian Government's current, vaguely stated, objective of ensuring national security. The primary aim of the UK Government appears to have been introduction of a scheme which enhances its ability to identify and record what its citizens do in their lives rather than one which allows people to reliably identify themselves. The LSE assessment of the UK Bill was that the only probable benefits would be in the area of social benefit fraud and in combating illegal workers. As it stands, it would be unlikely to reduce credit card fraud, immigration fraud, terrorism or money laundering activities. On the other hand, the UK identity card scheme is likely to significantly undermine citizens' rights under the Data Protection Act as well as some anti-discrimination legislation. The Act removes the individual's right of access and correction, lacks independent oversight of the technical and administrative arrangements, has no limits on how long data will be kept, and makes a presumption that all information collected is accurate.

The Australian Attorney-General has now removed the identity card debate altogether from the Federal Government's agenda, at least for the time being, apparently as part of Government strategy to proceed with the human services smartcard. Originally proposed as a way to reduce social

security fraud, the smartcard is already undergoing function creep and is to be used as a new Medicare Card, for the provision of all government services, for disaster relief and so on.

It is imperative that if a true national identity card is introduced again, the objectives of the scheme are precisely articulated so that there can be an appropriate evaluation of how the identity card would address those objectives. The need for a national identification scheme and identity card will have to be demonstrated compellingly and should not merely be an attempt to use one card to solve a range of identity verification and government fraud issues. The development of the proposed human services smartcard will be watched with interest to see if it is intended to be, or becomes corrupted into being, a national identity card.

References

Australian Privacy Foundation 2005, *Australia Card Mark II*, http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html#Mid2005 at 26/04/06.

Bajkowski, J, 'Centrelink and HIC thrown open to outsourcers in national smartcard push', Computerworld, 21 April 2005, http://www.computerworld.com.au/index.php?id=1607036145&eid=-255, at 24 January 2006.

Bajkowski, J, 'eCitizens to get single sign on', *The Australian Financial Review*, 30 March 2006.

Baker, R, 'Cabinet split over ID security', *The Age*, 22 April 2006, p1.

Caslon Analytics 2005, *The Australia Card and Beyond*, http://www.caslon.com.au/australiacard profile6.htm#terrorism, at 24/01/06.

Clarke, R , 'Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme', 5 *Prometheus* 1, June 1987, http://www.anu.edu.au/people/roger.Clarke/DV/OzCard/htm, at 24 January 2006.

Crawshaw, D, 'Ruddock rules out national ID card', *Herald Sun*, 26 April 2006.

Davies, S, 2004, *The Loose Cannon: An overview of campaigns of opposition to National Identity Card proposal*,

http://privacy.org.au/About/Davies0402.html at 15/11/05.

eGov Monitor Weekly, 'LSE clarifies ID Card cost claims', 22 November 2005, http://www.egovmonitor. com/node/3616, at 24 January 2006.

Federal Attorney-General's Department, 'Proposed Reforms to Australia's AML/CTF System', 16 December 2005, http://www.ag.gov.au/agd/www/agdhome.nsf accessed 16/12/2005.

Gratten, M, 'Smartcard to replace 17 others' *The Age*, 27 April 2006.

House of Lords Select Committee on the Constitution 2005, October, *Identity Cards Bill: Report with Evidence*, HL Paper 44, pp 6-8.

Howden, S, Crawshaw, D, Tasker, B, 'PM puts ID card firmly back on the agenda' *Sydney Morning Herald*, 16 July 2005.

Identity Cards Act 2006 (UK), http://www.opsi.gov.uk/ACTS/acts2006/20060015.htm at 1/05/2006.

Humphries, D and Todd, M, 'Identity Card Issue Returns', *Sydney Morning Herald*, 15 July 2005.

Identity Cards Bill 2005 (UK), http://www.publications.parliament.uk/pa/cm200506/cmbills/009/2006009. htm at 24/01/06.

Information Commissioner's Office 2005, *The Identity Cards Bill – The Information Commissioner's concerns* http://www.informationcommissioner.gov.uk/eventual.aspx?id=331 at 6/12/05.

Jackson, M, 2001, *Hughes on Data Protection Law in Australia*, LawBook Co.

Jordan, R, 2006, 'Identity Cards', *Parliament of Australia Parliamentary Library*, http://www.aph.gov.au/library/intguide/LAW/IdentityCards.htm, at 25 April 2006.

Lebihan, R, 'Citizen applicants may face biometrics check', *The Australian Financial Review*, 27 January 2006c.

Lebihan, R, 'E – passport loses face with privacy advocates', *The Australian Financial Review*, 21 February 2006a.

Lebihan, R, 'E – passports stuck in technical transit', *The Australian Financial Review*, 14 February 2006b.

London School of Economics 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, p 9, http://is.lse.ac.uk/idcard/identityreport.pdf at 11/11/05.

London School of Economics 2006, *The Identity Project Research Status Report* p 46, http://is.lse.ac.uk/idcard/identityreport.pdf at 20/01/06.

Out-Law News, 'General Election debate purpose of ID cards', 19 April 2005b, http://www.out-law.com/page-557 at 20/01/06.

Out-Law News, 'Information Commissioner voices ID card concerns', 17 August 2004a, http://www.out-law.com/page-4806, at 20 January 2006.

Out-Law News, 'ID Cards Bill survives House of Commons vote', 29 June 2005a, http://www.out-law.com/page-5859 at 20/01/06.

Out-Law News, 'Lords demand full costs of ID cards', 17 January 2006, http://www.out-law.com/page-6544 at 20/01/06.

Out-Law News, 'UK Privacy Watchdog Voices concerns over ID cards', 14 February 2004fb http://www.out-law.com/page-3329 at 20/01/06.

Priest, M, 2005, 'Ruddock to push national identity card', *Australian Financial Review*, 16 January 2005, p1.

Riley, J, 2005, 'ID card next on the agenda', *The Australian*, 29 December 2005.

Schubert, M, 2005, 'New smartcards could keep track of welfare', The Age, 21 April 2005, http://www.theage.com.au/news/National/New-smartcards-could-keep-track-of-welfare/2005/04/20/ 1113854259735.html, at 24 April 2006.

4

Community perceptions of biometric

technology

Suzanne Lockhart

Department of Criminology, University of Melbourne

Abstract

Biometrics is currently being used to enhance existing authentication mechanisms in the public and private sectors. Recent terrorist related events and an increase in identity related crimes indicate a probability that biometrics will become more widespread, however there has been little consideration of the social and cultural issues which will influence the community's response to the technology. This project examined community perception of biometric technologies and explored attitudinal barriers and motivators to the use and acceptance of biometric systems in Australia. Personality and social variables affecting attitudes to biometrics were identified and investigated in terms of the diffusion of innovation theory (Rogers 1995). A qualitative data collection method was employed which utilized a focus group methodology. Diffusion research centres on the conditions which increase or decrease the likelihood that a new idea, product, or practice will be adopted by members of a given culture. The project[2] also investigates how public and private sector organizations concerned with the implementation, adoption and diffusion of biometric technology might address identified concerns in order to increase the adoption of the technology.

Keywords: biometrics, community perception, social attitudes, adoption and diffusion

1 Introduction

Human identification is the process of associating a particular person with an identity (LoPucki 2001; Clarke 2001; Smith 1999). The process stems from a social context of belonging to a group or family where associates rely on memory to recognize peculiarities such as appearance, voice and shared knowledge. However, as identity transactions have moved from a social context towards being an economic necessity the process has become more complex. Globalization is a key driver and has affected many aspects of life including the transfer of information, goods

[2] This paper is an extract taken from Suzanne's published thesis, completed in fulfilment of a Master of Arts by research project in 2005 (M.A Criminology degree at the University of Melbourne).

and services, and people (Smith 2000). The requirement to prove identity is paramount in the day to day running of many organizations and it is generally acknowledged that many existing authentication mechanisms are unable to provide the level of security now demanded. Reliable authentication has the capacity to make many aspects of life operate more smoothly, make people more accountable for their actions and can provide a safer and more secure society.

It is evident that many countries are moving towards these enhanced identity infrastructures. Much of this activity is often attributed to rising concerns regarding terrorism but a direct response to terrorism is rarely the primary business driver. Some may argue that many countries are being compelled by international obligations and developments to adopt technologies such as biometrics however, these advancements have been part of long standing government initiatives which have only recently achieved financial and political momentum fuelled by terrorist acts. For leaders in the public sector the emerging debate over identity management and the selection of technology to authenticate citizens and businesses will be amongst the most important of all matters to shape the coming information age. The competing policy interests range from protecting citizens freedoms, privacy and other prerogatives on one end of the scale to ensuring law, order and national security on the other end. However the philosophical, social and political implications of implementing biometric technology solutions cut to the core of the relationship between government and citizen.

The Australian Government states that it intends to keep pace with the application of biometric technology to improve border protection, combat identity fraud, address passenger volume issues and meet international obligations. There may be many justifications for the use of biometrics however the public's perception and willingness to accept the technology may be quite a different matter. As stated by Rogers (1995) social or individual perceptions about innovations influence the degree to which the technology is adopted. To date there has been very little public debate or information dissemination on biometrics in the Australian public arena; the likely consequences of this being that any sudden change in government policy which requires the support of biometric technology stands to receive a high level of public and political criticism. Although

there may be biometric implementations such as e-passports which will be mandatory, careful analysis of biometric systems from the human issue perspective as opposed to the technical or infrastructural perspective should be paramount in order to improve the effectiveness, operational systems performance and ultimate adoption of the technology. Every biometric application will have different operational and user perspectives and it is a case of identifying and responding to those issues which will dictate a biometric applications success or failure (Ashbourn 2003).

There are many personality and social characteristics which have the potential to contribute to conscious or unconscious perceptions of biometrics. Perceptions will change over time and will be influenced by many societal, cultural, experiential and usability factors. This project aimed to identify and investigate human factor issues which may contribute to the formulation of perceptions of potential users of biometric technologies. Everett Rogers's diffusion of innovation theory was applied as an aid to inform and investigate the perception forming process of potential users and categorize identified issues. Rogers proposes that in the knowledge stage of the diffusion process the individual becomes aware of and constructs basics information about the innovation via receiver and social system variables. Personal and social characteristics, a perceived need for the innovation, social system variables and communication behaviour directly influence the degree of awareness and knowledge potential users may have about the innovation (Rogers 1995).

2 Overview of biometrics

2.1 Literature review

Biometric technology is an automated method of recognizing people based on physiological or behavioural characteristics which are measurable and distinctive to an individual (Coleman 2000; Churchill 2002; Smith 1999; Pankanti 2000; Cavoukian 1999). Physiological characteristics are either genetically inherited features such as; hair and eye color or phenotypic traits such as; iris, fingerprint and vascular patterns which are developed in the early embryonic stages, lead to

distinctive development and do not change significantly over time. Behavioural characteristics are learned or trained and identify patterns of usage such as handwriting or speaking. In theory these can be relearned or changed however this is difficult (Cavoukian 1999; Woodward, Orlans and Higgins 2003; Wayman, Jain, Maltoni, Maio 2005).

The technology has developed into a global industry of biometric based authentication systems covering various technologies including; fingerprint recognition, iris recognition; facial recognition; voice recognition, signature analysis and keystroke analysis to other esoteric systems such as facial thermography, ear lobe formation, gait, skin luminescence and brain wave pattern (Vogt 2002; Chandran 2002; Dunstone 2003). Unlike token and knowledge based approaches, biometrics has the ability to differentiate between an impostor and an unauthorized user. Biometric systems operate in two modes either; identification mode where the system identifies a person by searching a large data base of enrolled persons to locate a possible match (one to many, 1:N) and verification mode where the system verifies a persons claimed identity from their previously enrolled biometric (one to one, 1:1) (Woodward, Orlans and Higgins 2003).

This research project did not focus on an in-depth analysis of specific technical, human, physical or theoretical threats surrounding biometric acceptance. However it is acknowledged that the characteristics of ageing, gender, ethnicity, cost, health, security of information and standards, which are technical in nature, also have the potential to influence the way people perceive, interact and form opinions about biometrics, which will now be briefly discussed.

2.2 Technical threats

Technical threats refer to the failure or malfunction of equipment or software to carry out its function (Woodward, Orlans and Higgins 2003).

In terms of age this issue covers the physiological rate of change which might occur as part of the ageing process. Biometric traits generally remain constant except at either end of the ageing continuum. As the individual physically ages so too does the quality of their biometric data. For example, fingerprints may become worn, degeneration may occur within the eye and injuries on hands may take longer to heal. Individuals

enrolled on biometric databases as children will need to be re-enrolled as they mature to ensure continuity of template matching. Therefore, there is the requirement for systems administrators to consider appropriate stages when re enrolment should occur across the individual's lifetime (Ashbourn 2003).

In relation to gender there are two views to consider: the difference between male and female traits, and a possible difference between males and females ability to use biometric systems. Regarding traits it is obvious that there are several physiological differences such as hand size, face size and difference in voice waveform profile. Although these traits may affect the performance of the system, it does not suggest that physiological differences would affect the ability of the system to match a given sample. In fact, the degree of difference may be useful information to consider when the device is being built. With respect to usability there is the likelihood that females may confront more usability problems due to changes in hair style, fingernail length, cosmetics, plastic surgery, and jewellery and in some religions the wearing of face veils will invoke usability problems.

There are two perspectives to consider in terms of ethnicity. Firstly the question whether or not stored biometric data can discriminate between different ethnic groups in addition to being able to discriminate between different individuals. There is the view that different ethnic groups do have distinguishing features, particularly in relation to facial features and the fundamentals of voice and language patterns. However the ability of biometric systems to make these distinctions would require input and analysis involving anthropological data. Secondly, there is the perspective that there are different physiological properties between different ethnic groups such as voice, physical shape and size according to geographic location. Although more technical in nature these features may also influence the ability of specific individuals to enrol in biometric systems, such as iris recognition in populations where iris colour is uniformly dark.

Developments in authentication technology may be particularly alluring to many organizations however justification in terms of cost versus benefits is often foremost in most users' minds (Citizenship and Migration Canada 2003). System users are generally concerned about the cost of

implementing and maintaining technology in terms of creating higher institutional fees and higher cost for goods and services (Cox 2002). Giesing (2003) states that biometric systems should be available to everyone and that the cost needs to be acceptable to a large number of potential users and that it is equally possible that biometrics can result in lower long term costs such as those associated with replacing lost and stolen cards, passwords and personal identification numbers.

There are several issues relating to health which are likely to cause debate as biometrics becomes more widespread. Applied Security Technologies (2003) highlight two aspects, the first being direct medical implications which refers to the potential risk to the body arising from the use of biometric devices and the second as indirect medical implications which relates to biometric technology being able to reveal more about a person than their identity. This may include the user's state of health or psychological status. There is the concern that medical information may have the ability to affect life insurance and employment particularly if access to biometric information is shared across organizations (RAND 2002; UK Biometric Working Group 2002).

2.3 Human threats

Whilst organizations have a certain degree of control over the technical component of biometric systems the human component presents a peculiar set of problems which are often not realized until the system comes in to operation. Human threats can be internal or external to the organization and covers issues associated with unauthorized users and accidental or deliberate system misuse.

2.4 Physical threats

Physical threats to biometric systems include natural disasters such as fires, storm and water damage and also environmental conditions such as dust, lighting, moisture and humidity.

2.5 Theoretical threats

Theoretical threats include issue relating to algorithm vulnerability;

enrolment threats, physical or technical, system circumvention, spoofing, and biometric theft.

Whilst there are many other technical threats which should also be considered such as: data management issues; security of information, data sharing, interoperability, standards, accessing, data integrity, human rights, anti-discrimination, liability, auditing, and evidentiary requirements, an in-depth discussion of these issues is out of scope for this paper.

3 Personality and social issues affecting perception of biometrics

The justification for the use of biometrics may be evident to many organizations however the public's perception and willingness to adopt the technology is based on many personality, experiential, emotional and personality factors. Although potential users of the technology may be internal or external to an organisation similar issues will apply. After all the concept of biometrics will also be new to many administrative and operational personnel and in the majority of cases they will have very little or no experience of biometrics themselves to apply to the functions necessary to manage users and support the application (Ashbourn 2004; Moody 2003). This section details personality and social issues which will influence perceptions of biometrics and highlights the social implications associated with implementing biometrics.

3.1 Personality characteristics

The individual's emotional state at the time of interaction with the device will influence their perceptions of the technology. For example there are many emotions surrounding the reason for travelling. Airports for example are very volatile environments where people may be travelling for numerous reasons. They may be happy, sad, distressed, angry, nervous, intoxicated, affected by drugs or medication for example. All of these emotional states have the potential to influence the way individuals perceive and interact with biometric systems.

The ageing process may also affect the individual's psychological ability to logically understand what biometric technology is about, how it

works and the reasoning behind its implementation (Moody 2003). Similarly, many people suffer from psychological dysfunction which may influence their ability to interact with biometric devices. Apart from mental retardation, users may also be affected by personality disorders such as psychotic disorders; mood disorders; substance related disorders; anxiety disorders; dissociative disorders; impulse control disorders and adjustment disorders (Nevid, Rathus and Greene 2000).

3.2 Social issues

3.2.1 Privacy

Privacy is one of the most significant issues confronting not only the biometrics industry, but any organization which gathers personal information. The increasing implementation of biometrics raises questions about the technology's impact on privacy in the public sector, in the workplace and at home. Key aspects of privacy relate to both the individual and the organization. From the individual's perspective, privacy concerns arise in relation to the collection, choice, use, security of information and anonymity of the individual. From an organizational perspective, privacy issues concerning the manner and purpose of collection, solicitation, storage and security of information, access to records, relevance and the limits on use and disclosure of collected data are particularly relevant (Crompton 2002). Certain types of biometrics such as those where the user is asked to touch the device, engender a greater perception of privacy invasion and the potential for shared access to information and centralized databases raises concerns (Jain 2004; RAND 2003; Clarke 2002). Function creep or misuse of information refers to biometric data originally collected for one purpose, being used for another purpose (EKOS Research, 2003). Although using data for a secondary purpose may seem worthwhile, social issues arise when individuals are not informed of the purposes and have not given consent for the process (Rand 2003; Opinion Research Council 2003). Tracking which refers for example to the monitoring of spending and travel habits and screening which relates to covert surveillance and comparison to a watch list also challenges the individuals right to privacy. Biometrics also challenges the right to anonymity and the ability of those

in the legal system to take on a new identity. Another consideration is the impact of biometrics on the concept of social, personal and organizational trust.

3.2.2 Religion

Like many other forms of new technology biometrics forms the basis for fringe groups to promulgate millenarian or revelatory philosophies. Prevost (1999) and Rand (2003) state that religious groups argue that biometric authentication methods are the religious mechanism foretold in religious prophecy. Some Christians consider biometrics to be the brand as discussed in the Book of Revelation and other religious objections are based on the individual giving up part of themselves to a symbol of authority (Chuah 2002; UK Biometric Working Group 2002).

3.2.3 Education

Education, affluence and social structure in any society will also influence perceptions of biometrics and interaction with the technology. For example literacy levels will affect the user's ability to interpret or read instructions about how to use the biometric device and may also influence their ability to understand why biometric authentication methods are being implemented (Citizenship and Migration Canada, 2003; ORC, 2001).

3.2.4 Usability

In terms of usability a biometric system should be user friendly and provide rewards to the user in terms of convenience, efficiency and security. There are many other usability issues that are primarily technical in nature such as; being able to understand signage about operating instructions, ease of access and the degree of intuitiveness of the device which if not adequately addressed will make the system unattractive and socially unacceptable to the user (Giesing, 2003; Polemi, 1997; Chuah, 2003, Ashbourn, 2003; Brostoff and Sasse 2001).

3.2.5 Previous Experience

Previous exposure and use of information technology systems may also impact on the individual's level of comfort associated with using biometric devices. Those exposed to other authentication mechanisms, security issues and innovations may consider biometrics as a

technological progression and may enthusiastically accept the new innovation (Polemi, 1997). Orlikowski (1999) and Rose and Hackney (2000) discuss the use of information technology systems and suggest that it is the repetition of acts between and within groups and individuals in the community which causes the production of traditional ways of doing things. This tradition however can be easily changed as people either start to ignore them, replace them, reproduce them differently or when there are periods of marked social change (RAND 2002). It may be argued that the current global emergence and evolution of terrorist related events, proof of identity issues, technology and globalization signifies a current period of marked social change.

3.2.6 Victimisation

Prior victimization in relation to crimes of identity or fraud, particularly credit card fraud may also conceivably affect the victim's perception of biometrics. Those who have prior associations with law enforcement agencies as offenders or suspects and have had their fingerprints and photograph taken may view biometrics as an association with criminality (Polemi 1997; Ashbourn 2003).

3.2.7 Travel experience

Those people who travel frequently may view biometrics as security enhancing or may be sceptical about claims that biometrically enabled e-passports have the potential to assist and expedite the process of customs and immigration and increase air safety.

3.2.8 Disability/ health issues

Physical disability has the potential to be one of the major variables affecting personal perceptions of biometric systems. People with physical disabilities may find it difficult, confronting and discriminatory to use many biometric devices (Ashbourn 2003). Included are those with permanent and temporary disabilities such as those with wheelchairs, walking frames, artificial limbs, amputees, physical deformities, the blind and those using crutches. This also includes those with temporary illnesses and injuries such as those wearing eye patches, bandages, casts and those who may be suffering from a sore throat, laryngitis, arthritis, multiple sclerosis, Parkinson's disease or instability of the

eyeball or larynx (UK Biometric Working Group 2003). Similarly affected are those who undergo plastic surgery, either by choice or accident, or change their facial appearance by altering their hairstyle, growing beards or moustaches, wearing jewellery or face veils, using makeup and growing fingernails.

3.2.9 Environment

The immediate physical environment surrounding a biometric device has the potential to affect perceptions of the technology. For example, if the climate is cold people may need to remove gloves and hats in order to interact with the device. Other issues include the attractiveness and ergonomic design of the device, good signage and access for those with disabilities. Individuals may also have problems in respect of the use of biometrics in specific work environments. Organizations such as hospitals, abattoirs and food service industries require a high level of hygiene which may prove problematic for some biometric systems. In these situations people may not want to touch fingerprint sensors and may have concerns about removing gloves and protective clothing to access the biometric device. Another employment related issue concerns those employees who require hands free security access because they carry goods, wear protective clothing or are in industries where they have greasy or dirty hands.

Individual perceptions may also be influenced by the way people feel about interacting with technology in a public environment. Many people have experienced feelings of intimidation or embarrassment at ATM's or ticket stations caused by impatient people queuing at the machine, urging the user to hurry up. These situations may cause people to revert to familiar options such undertaking transactions face to face, using traditional passwords and personal identification numbers (Cox 2002).

3.2.10 Political issues

Political commentary relating to proof of identity, protecting national security, combating identity fraud and protecting the rights and privacy of the citizen will also influence perceptions of biometrics. Some argue that high integrity identifiers such as biometrics are a threat to civil liberty and a basis for ubiquitous and corporate identification schemes

providing enormous power over the population (Clarke 1994). Others consider that the fight against terrorism and other identity related crimes makes biometrics a valid response albeit a method which arouses emotive responses (Ashbourn 2003).

These factors illustrate the type and number of possible user issues which should be considered by any organization prior to considering the implementation of biometric based authentication mechanisms. If these factors are not considered there will be a high risk that the technology will not be accepted and the implementation will fail.

4 Theoretical framework

This research project applied Everett Rogers's theory of diffusion of innovation to biometrics to aid in the exploration, identification and conceptualization of issues, attitudinal barriers and motivators which may influence the way potential users of biometrics form their perceptions about the technology.

Diffusion research centres on the communication process through which a new technological idea spreads from one location or one social group to another. Every person reacts differently in the ways they hear about, understand and finally accept or reject an innovation. The diffusion process is a natural progression of people's attitudes, opinions and feelings towards accepting a new idea. Just because something is new it does not mean that it will be adopted automatically. The theory states that interpersonal contacts, information collected from the media and society also influence opinion and judgment. The theory centres on the conditions which increase or decrease the likelihood that a new idea, product or practice will be adopted by members of a given culture and that the decision to adopt or reject the innovation may change over time depending on new information received. Most innovation adoptions show an S shaped curve with the steepness of the S depending on the rate of adoption which is influenced by the characteristics of the innovation. Some innovations diffuse rapidly creating a steep S whilst others show a more gradual shape of the S curve depicting a slower rate of adoption (Rogers 1995). Other features of the theory consider that the innovation must have a

relative advantage, be compatible with other systems and past experiences, must be easy to use and should have qualities which can be tested and trialled with visible results. Rogers also highlights the importance of understanding the decision making and communication processes of potential users and the requirement to identify those users who will be early or late adopters of the innovation.

5 Methodology

This project used an exploratory method utilizing the diffusion of innovation theory as a working hypothesis. Data was examined to identify the validity of the theory to explain potential issues and processes which may influence biometric technology adoption in Australia.

A qualitative data collection method was employed utilizing focus group methodology. This enabled the researcher to examine: the participant's level of awareness and knowledge about biometric technologies, identify concerns individuals and the community may have about biometric technologies, identify attitudinal barriers and motivators to the use and acceptance of biometrics, and identify perceived issues and themes associated with the implementation of biometric technology. The discussion format remained flexible allowing exploration and open discussion to take place within the groups.

6 Results

Data indicated that the community acknowledges the dearth of information currently available to the public about biometrics. Many participants were familiar with the concept of biometrics however most stated that they had only seen biometrics on the television or in movies. To date the novelty of the technology, the limited availability of information and lack of awareness of biometric technologies has limited public debate relating to many aspects. Rogers (1995) observes that individual attitudes towards the usefulness of a new innovation are directly correlated with its extent of use. Data collected from participants in this project is largely congruent with Rogers' (1995) theory of diffusion of innovations. The data collected identified the direct and indirect experience that participants had

of biometrics, the activity and experiential processes whereby participants accumulated their knowledge about biometrics and individual emotional, physical and psychological variables which influenced their perceptions about biometrics. The following points were amongst those identified:

- strong opinion leaders in the focus groups were identified as those who were well educated, worked in the public sector, were business owners in the private sector and those who acknowledged the need to find solutions to address identity crimes.
- change agents were acknowledged as those organizations which already experience authentication and identity related concerns such as banks and secure installations. The innovation is biometric technology, which is perceived as having relative advantage by the majority of members in the focus groups.
- those participants who used traditional authentication mechanisms such as passwords and personal identification numbers welcomed the concept of biometrics to alleviate the requirements to remember multiple passwords and numbers and carry multiple cards.
- participants agreed that the level of knowledge about biometrics was low and that this should be addressed prior to biometric implementation to ensure users understand how the technology works, why it is being implemented and the advantages it will bring to the organization and its clients. Most participants had seen the use of biometrics in movies such as *Gattica* and *Mission Impossible*. Many participants were concerned about the health and safety aspects of biometrics however acknowledged that this was because they had little knowledge on how biometric systems worked.
- participants were sceptical about implementations which were not publicly debated.
- data indicated that it is necessary to undertake testing, evaluation and debate to counteract these issues and the technologies complexity because the technology brings with it issues relating to privacy, complexity, ease of use, storage, access, health issues and many other concerns.
- participants were comfortable about using the technology if it provided benefits and did not increase institutional fees.
- although privacy and data sharing was expressed as a significant

concern many participants were prepared to forego a degree of privacy to increase their physical and financial security.

- change agents should acknowledge that traditional fallback mechanisms need to be in place.
- age, education and technology awareness were the most influential variables. Elderly participants and those not familiar with technology were sceptical about their ability to access and use biometric systems. The necessity for training and public awareness was highlighted.

The results from this project substantiate that Rogers' theory of diffusion of innovation is a suitable theory to investigate and determine how people gather information about biometrics and how social and personality characteristics influence perception, adoption and acceptance of biometric technology. The theory validated issues identified in the authors literature review and provides a sample of current community perspectives concerning the implementation of biometric technology.

7 Conclusion

If researchers and change agencies could better understand the attributes associated with the biometric device products they are implementing and how the attributes relate to the extent of diffusion, they could incorporate this information in future program development and implementation strategies in order to maximize the impact of positive change in authentication mechanisms. Additionally if organizational structures which tend to inhibit diffusion are understood then change agencies and organizational structure could take positive measures to minimize the inhibitive impact. Rogers' framework enables a non linear user change process and the examination of the attributes of innovation factors which impact the extent of an innovations adoption.

Due to the personal interaction required between biometric technologies and the individual the author considers that the theory can be refined to state that the decision to adopt biometrics will also be influenced by the individual's physical status, psychological status, many experiential factors and influences from a social, national and global

context.

User participation and social acceptance is an essential process in the majority of biometric systems therefore it is imperative that any organization contemplating the introduction of biometrics identifies all stakeholders, considers how the subject, user and community might respond to the technology and identifies potential issues and solutions prior to program implementation in order to mitigate the risk of program failure.

References

Applied Security Technologies (2003). Health and Safety Issues in Biometrics. [On-Line]: Available: www.cesg.gov.uk/ast/index.cfm?menu

Ashbourn, J. (2003). Practical Biometrics. Typeset and Gray Publishing: London

Brostoff, A; Sasse, A. (2001). Computer Security: Anatomy of a Usability Disaster. [On-Line]. Available: www.andrewpatrick.ca

Cavoukian, A (1999). A Hegelian Basis for Information Privacy as an Economic Right. [On-Line]. Available: www-users.cs.york.ac.uk/~mdeboni/papers/Heglian_Basis_For-E-privacy.pdf

Chandran, V. (2002). Signatures as Biometrics. Biometric Institute Australia conference notes, October.

Chuah, L, (2002). The Future Challenges of Biometrics. [On-Line]. Available: www.giac.org/preactical/ LeeEhg.Chuah_GSEC.doc

Citizen and Migration Canada (2003). Traking Public Perceptions of Biometrics. [On-Line]. Available: Billie-Jo.Bogden@cic.gc.ca

Clarke, R (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. [On-Line] Available: www.anu.edu/people.Roger.Clarke

Clarke, R (2001). Biometrics and Privacy. [On-Line] Available: www.anu.edu/Roger.Clarke/DV/ Biometrics.html.

Churchill, J. (2002). SmartGate. Australian Customs Service. Australian Biometrics Institute Conference notes, October, 2002.

Coleman, S. (2000). *Biometrics: Solving Cases of Mistaken Identity*.

[On-line]. Available: http://global.umi.com.its-wu-ezprox2.lib.rmit.edu.au/pqd?Did=00000 00553

Crompton, M 2003) .Biometrics and Privacy. [On-Line]. Available: www.biometricsinstitute.org/bi/ cromptonspeech1.htm

Cox, L. (2002). Issues Regarding a Wider Use of Biometrics in the Financial Services

Sector. Biometrics Institute Conference, notes, October 2002.

Dunstone, T. (2002). Biometric Performance. Biometric Institute Australia conference notes, October.

Ekos Research (2003). Rethinking the Innovation Highway. [On-Line]. Available: www.ekos.com

Giesing, I. (2004). Biometric Perceptions. [On-Line]. Available:upetd.up.ac.za

IBIA International Biometric Association. (2002). Industry Notes. [On-line]. Available: www.ibia.org

Jain, A. (2004). Biometrics: A Grand Challenge. [On-Line]. Available: www.biometrics.cse.edu/biometrics agrandchallenge.pdf.

LoPucki. (2001). Human Identification Theory and the Identity Theft Problem. Texas Law Review, 80 (1) pp 98-135.

Moody, J. (2003). Public Perceptions of Biometric Device: The Effect of Misinformation on Acceptance and Use. [On-Line].Available: publisher@information.science.org

Nevid, J; Rathus, S; Green, B. (2000). Abnormal Psychology. Prentice Hall: Saddle River

Opinion Research (ORC), 2002. Public Attitudes towards the Use of Biometric Identification Technologies by Government and the Private Sector. [On-Line]. Available:

www.ap.uci.edu/appointments/NORC

Orlikowski, G. (1999). Awareness is the first and Critical Thing. [On-Line]. Available: www.dialogonleadership.org

Pankanti, S. (2000). Biometric Identification. [On-line]. Available: http://80-global.umi.com.its-wu-ezprox2.lib.rmit.edu.au

Polemi, D. (1997). Biometric Techniques. [On-Line]. Available: www.securityhotel.comg

Prevost, J. (1999). Biometrics with limited government intervention: How

to provide for privacy and security requirements of networked digital environments. [On-Line]. Available: www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.html

RAND (2003). Biometrics and Army. [On-Line]. Available: www.rand.org/publications/MR/ MR1237.sum.pdf

Rogers, E.M. (1995). Diffusion of Innovations (4th ed). The Free Press: New York

Roger, E.M; Scott, K.L. (1999). The Diffusion of Innovations Model and Outreach from the National Network of Libraries of Medicine to Native American Communities. [On-Line]. Available: http://nnlm.gov/pnr/eval/rogers.html

Rose, G; Hackney R. (2000). Towards a Structurational Theory of Information Systems: a substantive case analysis. Sent via email from the author – Jeremy@cs.auc.dk

Smith, R. (1999). Identity Related Economic Crime: Risks and Countermeasures. Trends & Issues in Criminal Justice, 129, pp1-6.

UK Biometric Working Group. (2003). Use of Biometrics for Identification and Authentication. [On-Line]. Available: www.cesg.gov.uk/site/ast/biometrics/me

Vogt, R. (2002). Research Direction in Speaker Recognition. Biometrics Institute Australia conference notes, October.

Wayman, J; Jain, A; Maltoni, D; Maio, D. (2005). Biometric Systems. Springer: New York.

Woodward, J; Orlans, N; Higgins, P. (2003). Biometrics. McGraw Hill: New York.

5

The social context of the security of Internet banking

Supriya Singh

Royal Melbourne Institute of Technology /Smart Internet Technology Cooperative Research Centre (SITCRC)

Abstract

This paper examines the users' perspective on the security of Internet banking in Australia within the social context. It supplements the technological and industrial approaches to security by drawing on user-centered research on banking in the Smart Internet Technology Cooperative Research Centre. We conclude that the most effective way to increase the perception of Internet banking security is to increase ease of use, convenience, personalisation and trust. Without the perception of security, there will be little trust in banking and transactions on the Internet. This will impede aspects of the nation's critical infrastructure.

Keywords: Internet banking, security, users' perspective, trust, privacy

1 Introduction

Banks want customers to feel Internet banking is secure, so that Internet transactions can substitute for a greater part of the more costly

branch, telephone, ATM and EFTPOS transactions. Internet banking is now an integral part of banks' business model. Banks also want to retain the mantle of a trusted organization and Internet sites. In the United States, banking sites are trusted by 68 per cent of all Internet users and more so by those who use Internet banking (Princeton Survey Research Associates International 2005). Not achieving this perception of security will have the wider effect of reducing customers' trust in banks, electronic banking and more particularly Internet transactions. It is however impossible to ensure perfect security, particularly as the unsupported PC was not designed for secure Internet commercial transactions (Adamson 2003). PC manufacturers and suppliers of related products have clearly stated that the unsupported PC is not suitable for home banking. This is even more true as criminal attacks on Internet banking have become more sophisticated, particularly with the development of key logger software (Adamson 2003; McCullagh and Caelli 2005).

Banks addressed the problem of imperfect security in the case of credit cards by capping customers' liability in case of fraudulent use. For e-commerce transactions that involve purchase and sale, banks in Australia have laid the responsibility of fraudulent use on the merchants. Bank contracts with customers however, are ambivalent about the responsibility for the security of Internet banking transactions. Banks are active in moving customers to Internet banking through lower fees and bank branch closures, while at the same time also warning customers of the need to be careful. Though Australian Standards relating to Electronic Funds Transfer and the EFT Code of Conduct provide consumer protections, the protections for Internet banking have still to be tested in court. It is believed the National Australia Bank reimbursed one of its customers whose Internet banking from a cyber café was intercepted by a Trojan key logger (McCullagh and Caelli 2005).

The first case testing the responsibility for the security of Internet banking is pending in the Florida State Court. (There has been no further news since May 2005 of it on the Internet in terms of commentary). This case is important for it will establish for the first time whether the responsibility for security of Internet banking lies with the customer or the bank. In April 2004, AHLO Inc a small printer and ink business in Miami, lost US$ 90,348.65, in a Bank of America account through a fraudulent

transfer from the company's account to an account with the Parex Bank in Riga, Latvia. AHLO alleges it advised BOA, but the bank did not take action for some 19 hours. By this time $US 20,000 had been withdrawn from Parex Bank. BOA argues that it does not have the authority to have the remainder transferred to AHLO. AHLO is proceeding against the bank alleging in part that there has been a breach of fiduciary duty and that the bank has not acted in good faith. BOA is arguing that the problem lay with the security of AHLO's PC rather than its own networks and so the responsibility rests with AHLO. The Secret Service was called in and found that AHLO's computer was infected with the Trojan called Coreflood, though does not say it was the cause (Leyden 2005; McCullagh and Caelli 2005).

There are divided opinions as to the bank's responsibility. The bank may win the case, but denting consumer confidence makes the bank's legal strategy questionable. Making small businesses responsible for the technical security of the PC may not be a viable option. On the other hand paying out AHLO may open the floodgates (Sraeel 2005). Ramasastry, a former staff attorney for the New York Federal Reserve Bank, wrote that "The legal duty of banks to protect against hacking should be limited to their own networks - about which they are knowledgeable, and over which they have control" (Cocheo 2005). The AHLO case may be won or lost on issues of technical security of the business PC or the bank's responsibility for fraudulent Internet banking. But in the meantime Lopez, the owner of AHLO "has stopped using wire transfers" (Leyden 2005).

This is the background of the inherent conflict between the near impossibility of customers ensuring the ongoing and continuous security of the PC against advanced malware, and banks' policies relating to security. The story gets more complicated as one goes beyond technology and the law to take into account users' perspectives on Internet banking security. In section two I survey the developing literature on user-centred security. In section three I draw upon a qualitative user-centred study of banking. In section 4, I conclude that customers' perception of security is increased by addressing issues of trust, usefulness and personalization.

2 User-centred perspectives on security

The user-centred approach to security is in its early stages. There are three strands to the debate. The first is that it is the usefulness of technology for a designated activity rather than technology itself that is at the centre of security. The second is to move from a focus on security to an emphasis on trust. Control and comfort with the transaction, together with a perception that the customer is being looked after, is essential for trust. The third is the close connection between privacy and the control of personal information. This emphasis on control of personal information connects security, trust, privacy, and identity.

2.1 Usefulness and security

The connection between usefulness and technology is the thrust of much of the developing user-centred perspectives on security. This connection focuses on three aspects: the primacy of the activity over technical aspects of security, usability of security solutions, and users' feelings of control.

Karat et al (Karat, Karat et al. 2005) point out the primacy of the activity, saying "... the use of security and privacy solutions is generally not the user's main goal. Users value and want security and privacy functionality as secondary to completing their primary tasks" (p. 2).

There is also a narrower focus on the usability of security solutions. Schneier (2000) opens his book Secrets and lies: Digital security in a networked world with a *mea culpa* relating to his earlier text on applied cryptography. He says he was wrong to think that mathematics alone could ensure digital security. He did not take into account users and their context (Schneier 2000).

He says security is a multi-layered process, rather than a product. Reflecting on his earlier influential work, Schneier says,

> I came to security from cryptography, and thought of the problem in a military-like fashion. Most writings about security come from this perspective, and it can be summed up pretty easily: Security threats are to be avoided using preventive countermeasures" (p. 397).

He realised in 1999 that "…the fundamental problems in security are no longer about technology; they're about how to use the technology" (p. 398).

D'Hertefelt (D'Hertefelt 2000) also argues "that the feeling of security experienced by a user of an interactive system does not depend on technical security measures alone. Other (psychological) factors can play a determining role" (no page number). This research suggests that "[t]he feeling of security experienced by a user of an interactive system is determined by the user's feeling of control of the interactive system."

Based on qualitative research towards making the website of an European airline more usable, they came up with the unexpected finding that "people's perception of security when doing on-line transactions depends on the simplicity of the site and on the availability of user support." D'Hertefelt says

> This observation puzzled us. Discussions about security on internet seem preoccupied with technical issues such as 128-bit encryption, secure sessions, authentication, digital certificates, secure sockets layer, etc. And we observe that people feel secure because... "it's easy"?

One approach which bridges the gap between security and usability is "the concept of integrated user-centered security engineering" (Gerd tom Markotten 2002). Their investigation of existing security tools, like PGP (www.pgp.com), Signtrust Mail (www.signtrust.de), and freedom (www.freedom.com), showed that systems do not fail because of malfunction, but because they were too complex or difficult for users. The need was for "usable security" combining the processes of usability and security engineering.

2.2 Trust and security

Trust is a wider concept than security. Trust however is difficult to define because it is nebulous and all pervading. People speak of trust most clearly when they speak of a lack of trust. This is especially so in situations where there is a greater risk and where information is less easily available (Singh and Slegers 1997). Issues of trust and the use of electronic money are increasingly being discussed (Luhmann 1988; Singh and Slegers 1997; Lee and Allaway 2002; Suh and Han 2002; Hsiao 2003; Barr, Knowles et al. 2004; Liu, Marchewka et al. 2004).

It is important to disentangle the concepts of security and trust, because even "usable security" is not always a sufficient condition for

trust. David Bollier (1996), reporting on the discussion of the Aspen Forum on Electronic Commerce (Bollier 1996, p. 21) , distinguishes between “issues of ‘hard trust,’ which involve authenticity, encryption, and security in transactions, and issues of ‘soft trust,’ which involve human psychology, brand loyalty, and user-friendliness” (p 21). Singh and Slegers (1997) unpack issues of soft trust and electronic money. They conclude that the user has to feel he or she is in control of the information, that he or she has comfort in the use of the service or channel. The dimension of caring is particularly important as a glue for trust in all cases, but particularly where the user does not have the expertise or ability to control the situation.

2.3 Privacy as the control of personal information

Lawyers, technologists, sociologists and psychologists have defined the concept of privacy in different ways. In the user studies on the control of personal information conducted in the Smart Internet Technology CRC, we have found that privacy is seen as the control of the sharing of personal information and control over the representation of ourselves. Privacy did not equate with anonymity. It also did not mean being left alone (Singh and Cassar-Bartolo 2004). This emphasis on control of the sharing of personal information and presenting our version of ourselves, connects security, trust, privacy and identity. Karat et al (Karat, Karat et al. 2005) say

> The intersection of human-computer interaction (HCI), privacy and security is emerging as a critical area for research amid the backdrop of recent world events. .... it is becoming increasingly clear that really making our systems secure and enabling appropriate attention to privacy issues will require more than just a technology focus (p. 1).

Issues of privacy in the banking context focus strongly on the risk of losing money via the fraudulent use of the credit card and/or information related to Internet banking. As banks hold detailed personal information about a person’s financial status, there is the additional worry that a leaking of this information could affect a person’s representation of self and also lead to spam.

In the next section I draw on a qualitative study of Australian consumers’ perceptions of security within the context of how they bank.

3 Qualitative study of privacy and security in Australian banking

The aim of the qualitative study was to understand how Australian consumers perceived issues of security, identity, trust and privacy in banking. The study adopted the users' perspective where the emphasis was on the banking activity. I am reporting on the interim results of the study, drawing on open ended interviews with 38 people in Melbourne and Brisbane, between April 2005 and September 2005. The people were accessed through personal and professional networks. Our sample had nine men and 29 women; an even distribution across ages; a range of annual household income levels; a dominance (30 of 38) of those with a BA or higher degree, particularly in IT.

We chose the qualitative "grounded" approach for we needed to understand how people manage their financial information across life stages (Glaser and Strauss 1967). We used N6, a computer program to assist and display the rigour of qualitative analysis (Morse and Richards 2002).

3.1 Usefulness, convenience and security

Usefulness and convenience were the main factors leading to the use of Internet banking for 19 of our 38 participants. Two did not use Internet banking for they did not find it useful enough. Of the other 17 people who did not use internet banking, 13 had an annual household income of less than AUS$50,000, hence the issue was one of access and affordability. Four did not use Internet banking because of a lack of security.

Fifteen of the 19 who used Internet banking valued convenience and habit over concerns about privacy and security. They used a number of strategies to direct attention away from their not being totally satisfied with the security and privacy of the Internet. They tried not to think of the risks because they felt they could not control these risks. They also used risk minimization strategies such as using credit cards with low limits, using a computer and network they saw as secure, or assuring themselves that the site had the sign of a lock to symbolize security.

Ellen, 35-44, an academic in part time work and a household income of over $100,000 says she likes the convenience and the immediacy of the

Internet. She buys groceries online and does all her banking on the Internet. She thinks that hackers are going to be able to steal their money one day, “but at this stage I don’t see it as a security problem.” She tries to be careful by keeping the passwords secure, making sure she is on a secure site. She sees the university server as secure. In the end she tries to stop being anxious by saying nothing is totally secure. And if anything happened she has the confidence to follow up and get the money back.

Laura, 25-34, with her own business in health services, has always banked using the Internet. Replying to questions about trust, privacy and security, she says,

I don’t know that I think about it a lot, because I think I don’t understand it enough. So I don’t think about it. … It’s completely hiding your head in the sand.

Others like Gillian, 35-44, a PhD student in IT and a household income of more than $100,000, try and protect themselves by using the latest spyware, or having a credit card with a very low limit. She trusts the bank’s system “is secure”.

3.2 Trusting the bank

There is a comfort in dealing with the bank in a way that offers convenience and a greater control of current information about one’s money. But when the untoward happens, and the bank deals with the customer in a way that he or she finds caring, then the trust is often further enhanced. Three of our 38 participants have experienced the fraudulent use of the credit card. Two of the three continue to use Internet banking because their problems with the credit card were satisfactorily resolved.

Anita, now a housewife, 55-64 with a household income between $55,000 and $74,000 says $300 was withdrawn from her husband’s credit card. When he rang the bank – for he was the primary card holder – the money was returned. This experience left Anita cautious about checking statements and she does not use the credit card on the Internet – choosing to use BPay. However, she regularly uses the Internet to monitor her accounts, transfer money and pay bills. She uses the Internet but worries about the security and keeps a constant eye on her finances. Her only strategy to lessen the risk is that of constant monitoring. She says, “I just hope that… nothing will happen. I just put… full trust on... the

banks that.. they are doing their best…"

Amber, 28, with a household income below $50,000 says her partner had money taken from his credit card. He rang the bank and they put the money back. This experience of fraud with the credit card and its subsequent solution has gone to enhance the feeling of trust in the bank. Dora, 35-44, an academic also had a problem with the fraudulent use of her credit card when in South East Asia. She says this is one of the reasons she doesn't use Internet banking.

3.3 Privacy, personalisation and responsiveness in the bank

For our participants, comfort in the privacy of personal information with the bank, was not based on the legal privacy policies. Only three of the 38 people in our sample read the privacy policy. For the most part the participants felt they could not hold the bank to account because of the privacy policy. Three others saw it was the bank that used the Privacy Policy as a way to restrict their access to information and personalise their accounts. This was particularly the case with joint accounts, where the bank imposed a hierarchical structure of the primary and secondary account or card holder. It was the primary account holder who had the right to change account information. The bank's actions did not take into account the wishes of the couple themselves, for more equal control.

Gillian, 35-44, a PhD student in IT, with a household income between $75,000-$99,999 said she and her husband found themselves in the awkward situation where the bank would not accept her changing the contact details for the credit card for both herself and her husband. She is the one who has the online log-on for the credit card. This is so that they can minimise the number of passwords they have. She says she emailed and asked

> …to change our address, our postal and home address because we had moved. They changed mine but they wouldn't change his, even though I'm a secondary card holder.

This meant her husband had to ring the bank to give Gillian permission to change the credit card details. She tried to find out if she could change the details in the future and the bank said "No. Every time you want to make any changes, he has to ring and authorize you to talk to me again."

Gillian says,

> All we had to do was tell his name, his date of birth, his mother's maiden name and the account number….If you knew the person you could quite possibly know the mother's maiden name. …To me that is not as secure as being able to send an encrypted email through a banking system. There is no point fighting them. They don't listen.

4 Conclusion

In this paper I have drawn on three strands from the nascent literature on user-centred security, trust and privacy. People focus on a designated activity such as banking, rather than the technologies used to enhance security. Trust in the organisation or the medium is at the centre of people's feelings of control and comfort. Users' perception of control also is at the centre of issues of privacy. These arguments from the literature are supported by interim results from a qualitative study of identity, trust, privacy and security in banking. Convenience and ease of use are at the centre of customers' positive experience of Internet banking. The usefulness of Internet banking together with trust that the bank will look after customers' interests, overcomes concerns about security and privacy. The concerns with Internet banking rest more on customers' perception of inadequate control over their personal information and personalisation of banking.

The literature and the qualitative study leads to the conclusion that banks can increase customers' perception of security in three ways. The first is to increase convenience and usefulness of Internet banking. The second is to enhance trust in the bank by having customers believe the bank will not allow them to suffer fraudulent transactions. The third step is to give customers a more personalised experience of Internet banking by giving them greater control of their transactions and information. Focusing on technical issues of security that customers cannot completely control may move everybody the Lopez way, away from Internet banking.

References

Adamson, G. 2003, The Mixed Experience Of Achieving Business Benefit From The Internet -A Multi-Disciplinary Study, *Business*

Information Technology, RMIT University, Melbourne. http://adt.lib.rmit.edu.au/adt/public/adt-VIT20041105.112155

Barr, T., A. Knowles, et al. 2004, Taking users up the value chain: Australian Internet research, Smart Internet Technology Cooperative Research Centre, Melbourne.

Bollier, D. 1996, The future of electronic commerce: A report of the Fourth Annual Aspen Institute Roundtable on Information Technology, The Aspen Institute, Aspen, Colorado.

Cocheo, S. 2005, Privacy rumblings grow louder: prompted by recent publicity over data breaches, Congress, state houses, and, increasingly, the courts are considering cases and proposals that could impact banks., ABA Banking Journal, http://www.allbusiness.com/periodicals/article/455368-1.html accessed 30 January 2006

D'Hertefelt, S. 2000, Trust and the perception of security, http://www.interactionarchitect.com/research/report20000103shd.htm accessed 23 June 2004.

Gerd tom Markotten, D. 2002, User-Centered Security Engineering, http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/publications/Ge2002.pdf accessed 10 October 05

Glaser, B. G. & A. L. Strauss 1967, *The discovery of grounded theory: Strategies for qualitative research*, Aldine, Chicago.

Hsiao, R.-L. 2003, "Technology fears: distrust and cultural persistence in electronic marketplace adoption," *The Journal of Strategic Information Systems*, 12,(3), pp.169-199.

Karat, C.-M., J. Karat, et al. 2005, "Why HCI research in privacy and security is critical now," *Human-Computer Studies*, 63, pp.1-4.

Lee, J. & A. Allaway 2002, "Effects of personal control on adoption of self-service technology innovations," *Journal of Services Marketing*, 16,(6), pp.553-572.

Leyden, J. 2005, Florida man sues bank over $90K wire fraud, The Register, http://www.theregister.com/2005/02/08/e-banking_trojan_lawsuit/ accessed 30 January 2006.

Liu, C., J. T. Marchewka, et al. 2004, "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce,"

Information & Management, 42,(1), pp.127-142.

Luhmann, N. 1988, 'Familiarity, confidence, trust: problems and alternatives', in *Trust: Making and Breaking Cooperative Relations*, ed D. Gambetta, Basil Blackwell, New York**,** pp.94-107.

McCullagh, A. & W. Caelli 2005, *Who goes there? Internet banking: A matter of risk and reward*. ACISP 2005, Brisbane, Springer-Verlag.

Morse, J. M. & L. Richards 2002, *Readme First for a User's Guide to Qualitative Methods*, Sage Publications, Thousand Oaks, Calif.

Princeton Survey Research Associates International 2005, Leap of Faith: Using the Internet despite the Dangers, http://www.consumerwebwatch.org/pdfs/princeton.pdf accessed 30 January 2006

Results of a National Survey of Internet Users for Consumer Reports WebWatch, Consumer Reports WebWatch, New York.

Schneier, B. 2000, *Secrets and lies: Digital security in a networked world*, John Wiley & Sons, New York.

Singh, S. & K. Cassar-Bartolo (2004). *The privacy of money and health*. OZCHI, Wollongong.

Singh, S. & C. Slegers 1997, Trust and electronic money, Centre for International Research on Communication and Information Technologies, Melbourne.

Sraeel, H. 2005, Lopez v. BofA: Bad Press Or Precedent Setting?, USBanker, http://www.us-banker.com/article.html?id=20050401HUQ7QVJB accessed 30 January 2006.

Suh, B. & I. Han 2002, "Effect of trust on customer acceptance of Internet banking," *Electronic Commerce Research and Applications*, 1,(3-4), pp.247-263.

6

The importance of utilising electronic identification for total farm management in Australia

Adam Trevarthen

School of Information Technology and Computer Science, University of Wollongong

Abstract

This paper aims to explore how Radio Frequency Identification (RFID) can be utilised on dairy farms to enhance total farm management. There is a growing worldwide trend for countries to implement whole-of-life traceability systems for livestock, and RFID is clearly the dominant technology being chosen to achieve this aim. In line with this global trend, and to meet the requirements of key trading partners (such as the EU), Australia has implemented the National Livestock Identification System (NLIS) to provide whole-of-life traceability for livestock– a system based on the use of RFID devices. As such, it is proposed that dairy farmers utilise RFID so as to not only comply with NLIS requirements, but to extend the use of RFID onto their farms so as to provide additional benefits for themselves through subsequent enhancements in farm management practices.

Keywords: radio-frequency identification, livestock, traceability, total farm management

1 Introduction

Radio Frequency Identification (RFID) is becoming globally recognised as the technology to implement animal identification, and has become a mandatory form of livestock management in many countries (such as Canada, and some states of Australia), while other countries have begun trials of the technology (such as the United States of America). In the current global livestock environment, awareness, fear and recognition of animal borne diseases such as 'mad cow disease' have driven calls for reliable and effective systems for individual identification and tracking of livestock throughout the animals' entire lifecycle. Such systems empower authorities with rapid and precise information (such as the animals' farm of origin, cows it has been in contact with etc.), aiding them to take prompt and direct action to reduce the possibility of a disease outbreak. Considering this global trend towards the use of RFID for individual whole-of-life animal tracking, it appears that farmers will soon be utilising this technology, whether by choice or to meet a mandatory/obligatory requirement. As such, it is important that research be undertaken to identify how the electronic identification technology of RFID may be utilised to enhance total farm management, derive additional benefits and maximise return on investment for the farmer.

2 Background

2.1 What is RFID?

RFID is defined as "… a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves" (RFID Journal 2005a). This technology is commonly implemented using a system of reusable and programmable RFID tags (also known as transponders) and readers (also known as interrogators). These tags can be attached/built-in to virtually any good/object and provide a storage capacity of up to 2 kilobytes of data (RFID Journal 2005a). This allows more than just a unique identifier to be stored on the tag, but may also allow additional information pertinent to the object to be stored (such as expiration date, manufacture date, owner information etc.). The receiver

can be a mounted or hand-held computer-controlled device, and when a tag is brought within the reading range of a receiver, the receiver captures the data stored on the tag and forwards this to the host computer (Ames 1990, p. 1:5; RFID Journal 2005a; Williams 2004).

2.2 Characteristics of RFID – active vs passive tags

There are two main forms of RFID tags – active and passive. The primary difference between the two is that active tags have their own power source (typically a battery), and also incorporate a transmitter to enable communication, whereas passive tags do not. This power source provides active tags with a greater and more reliable read range, as well as greater data storage and transfer capacity than their passive counterparts. Active tags however, are significantly larger than passive tags (currently, the smallest active tag is approximately the size of a coin) and also come at a much higher cost. Active tags usually operate at frequencies of 455 MHz, 2.45 GHz, or 5.8 GHz, and have a typical read range of about 20 to 100 meters (RFID Journal 2005c).

Instead of utilising their own power source and transmitter, passive tags generate enough power from the RFID reader's signal to transmit their information. They do this by manipulating the energy (radio waves) sent from the reader, simply reflecting the energy back to the reader in a manner that the reader can interpret into data. Not incorporating a power source or transmitter enables passive tags to be much smaller (in 2004, the smallest commercially available device was 0.4mm x 0.4mm and thinner than a sheet of paper) and also dramatically cheaper. Sacrificing the power source however, means that these tags have a shorter read range, and cannot store as much information (Hecht & Hecht 2004; Ames 1990, pp. 1:15-16; RFID Journal 2005b). Passive tags operate at a range of frequencies, primarily low frequency, high frequency, and ultra-high frequency. Low frequency tags operate at 124kHz, 125kHz, or 135kHz, and have a read range up to 0.33 meters. High frequency tags operate at 13.56MHz and have a read range of up to one meter. Ultra-high frequencies operate anywhere from 860MHz and 960MHz, providing a read range of up to 3.3 meters (RFID Journal 2005b).

2.3 Advantages of RFID

RFID provides many advantages over other electronic identification technologies such as barcodes. These advantages include the ability to store more information, strong machine readability, fast read speed, and having no operating costs once implemented. Further, as their usage relies upon radio waves rather than line-of-sight technology, RFID tags do not need to be visually seen to be read – they simply must enter the scanning field of the reader. This therefore dramatically increases ease of use, as well as providing greater reliability in light of general wear and tear, and environmental elements such as dirt and dampness (Finkenzeller 1999, pp. 6-8). Such elements may render other line-of-sight identification technologies such as barcodes unreadable. Consequently, RFID systems have a wide range of applications in a number of industries.

2.4 Animal identification and RFID

Animal identification is one of the most common applications of RFID technology, and one that has been pioneering the technology for almost 20 years (Accenture 2005; Finkenzeller 1999, p. 245). Focussing on the livestock industry, there are four main ways in which RFID can be used for animal identification – attaching a transponder to the collar, attaching a transponder in a tag form to the animals ear (similar placement to current ear tagging however utilised vastly differently), injecting tiny glass transponders under the animal's skin, or via a 'bolus' where the RFID transponder is mounted within an acid resistant, cylindrical housing which is inserted permanently within the animals stomach (Finkenzeller 1999, pp. 245 – 250).

2.5 RFID for traceability and farm management

There is currently a worldwide trend towards improving traceability systems within livestock industries, and RFID is the primary technology of choice. Spurred by disease incidents from around the world, such as the Bovine Spongiform Encephalopathy (BSE, more commonly known as 'mad cow disease') outbreaks in the late 1990's, countries such as those within the European Union (EU) have enacted policies to ensure livestock can be traced through their entire lifecycle (Animal Health Australia n.d.).

Programs such as these are designed to minimise or eliminate the spread of disease as authorities are able to trace origins of diseases, identifying farms and animals that may have been affected and subsequently they are able to take direct appropriate action to minimise further spread (Food Production Daily 2004). Other countries such as Canada have enacted electronic identification legislation requiring all livestock to be tagged with approved RFID devices by September 1, 2006 (CCIA 2005), while America is currently operating voluntary trial operations utilising RFID tags as they consider a full individual animal identification proposal (Animal Health Australia n.d.; Goth 2005).

2.6 Focus benefit of RFID

An important benefit listed above is that of offering producers improved herd management options. As the global push towards mandatory RFID identification and whole-of-life traceability systems continues, it is proposed that farmers should take advantage of this situation, and extend the usage of this technology to enhance farm management practices. This research will investigate this concept and attempt to derive a possible ideal framework for the use of RFID technology for total farm management.

3 Literature overview

An abundance of literature is available regarding the technology of electronic identification, with its application for animal identification included as a topic in much of this literature. Entire websites such as RFID Journal (2005c), AIM Global (the Association for Automatic Identification and Mobility) (2005), RFID News (2005), RFID Times (2005), and many more sites are dedicated to electronic identification, providing an abundance of information, international news stories and developments regarding both the technology and the industry, including its applications for animal tracking. Authors such as Finkenzeller (1999) and Gerdemen (1995) devote entire books to the subject of electronic identification and RFID, while Finkenzeller (pp. 245-252) also briefly demonstrates its usage for the purposes of animal identification and tracking.

The major authors in this field are Geers et al. (1997), who devote an

entire book to electronic identification, monitoring and tracking of animals. Providing information on current animal tracking technology, how they work, current applications, and possible future direction, Geers et al. demonstrate the growing awareness and importance of electronic identification for farm management. Considering improved disease and fraud controls, combined with the desirable and dominant cost-benefit ratio that can be derived from the utilisation of electronic identification for farm management, Geers et al. (pp. 26-28) provide a clear message that electronic identification is the likely path of animal identification in the future.

Michael's thesis (2003) further supports this view, providing an in-depth review of a wide variety of electronic identification technologies (including smart cards, barcode and biometrics). A section of chapter seven, regarding animal identification using RFID demonstrates that traditional forms of animal identification are considered inferior in comparison to RFID technology, while the application of RFID identification to improve farm management practices is also touched upon (pp. 239 - 240). Karnjanatwe (2005) provides an insight into an actual application of RFID technologies used to enable enhanced farm management of pigs, such as automating the feeding process and regulating how much each pig eats. Ishmael (2001) tells of the economic benefits achieved by a group of farmers resulting from utilising RFID technology to provide individual identification and subsequently enhanced farm management operations on their beef farm in America. James (2004) states how electronic identification can be used to reduce the labour required for the milking process, providing large cost savings, while Davies (1997) demonstrates the ability to improve the quality of milk yields through controlled feeding processes based on electronic identification. This literature demonstrates the rising recognition of electronic identification for animal identification and farm management practices, while also demonstrating that it does have practical applications for farm management and the ability to provide economic benefits for farmers.

4 Benefits of using RFID for farm management

4.1 Financial and managerial benefits for the farmer

The first reason is for increased profitability for the farmer, and assistance with managerial procedures on the farm. Geers et al. (1997) note that despite electronic identification of farm animals being more expensive than traditional forms of identification, it allows for a faster payback on investment through exploiting a wider range of possible applications. Identification can be used to facilitate control activities on farms, including:

> "... follow-up of premiums, milk-record control, tracing back of transit and disease prevention, progeny testing and herdbook administration, electronic feeding stations, automatic gating in group housing facilities, accountability to markets and slaughterhouses, animal health control, public health control, animal welfare surveillance, prevention of fraud, tracing back of stolen stock, facilitating trade, central database facilities" (Geers et al. 1997, p. 39).

Geers et al. continue, stating that in the modern farm environment, farming needs to manage more animals to be cost-effective. Consumers also have an impact on what farm management should be, and subsequently, management processes become increasingly difficult for the farmer. Electronic identification can strongly aid a farmer in their managerial efforts, while also deriving financial benefits from exploiting an increased range of possible applications.

4.2 Worldwide trend for traceability

A second primary driver for the move to RFID for farm management is to conform to the current worldwide push to introduce individual whole of life tracking programs for livestock.

In the wake of recent disease outbreaks amongst livestock (such as 'mad cow disease' and foot-and-mouth disease), countries around the world are implementing policies and procedures to ensure individual whole-of-life traceability for all livestock. RFID is the technology of choice for these solutions. Countries such as those within the European Union

have enacted policies to ensure livestock can be traced through its entire lifecycle (Animal Health Australia n.d.), Canada has enacted legislation requiring all livestock within Canada to be tagged with an approved RFID device by September 1, 2006 (CCIA 2005) and America is currently operating voluntary trial operations utilising RFID tags while considering a full animal identification proposal. (Animal Health Australia n.d.; Goth 2005). Rizoli (2003) notes that trials of RFID technology for identification and tracking of livestock have been taking place in America since 1998, when the National Farm Animal Identification and Records (National FAIR) pilot project was launched.

4.2.1 Purpose of the programs

These whole-of-life traceability programs are designed to record and present accurate and up-to-date information regarding all cattle movements. Such systems enable authorities to rapidly trace the origins of any cattle diagnosed with a serious contagious disease (should one ever occur), identifying farms and animals that may have been affected, or even been the source. Subsequently, they are able to take direct appropriate action to minimise further spread (Food Production Daily 2004). Rizoli (2003) further notes that such traceability systems are required so as to reduce the possible impacts of a terrorist attack upon the livestock industry. Rizoli quotes National FAIR Director Robert Fourdraine as stating in regards to terrorism that,

> "One outbreak of disease (among livestock) can be isolated and contained… But if someone were to introduce foot-and-mouth disease in several different places at once it would shut down the food supply".

This viewpoint is also recognised by Nagl et al. (2003), and raises an interesting point and benefit of the current systems being implemented.

4.2.2 Infeasibility of traditional identification methods

Geers et al. (1997, p. 26 - 27) notes that traditional identification methods certainly could not provide the reliability and accuracy being sought by current requirements. Traditional ear tags are reported to be lost 5 to 60% (Aarts et al. 1992) of the time, while brands or tattoos on cattle can be damaged or fade away. A further key drawback of such traditional systems is that they require visual detection and must be recorded manually, which can easily introduce human errors, while the

labour cost of such a practice is also high. Reading errors are estimated to occur in six of every 100 animals processed via traditional mechanisms, while electronic devices are estimated to produce only one error for every 1000 animals (Austin 1995 quoted in Geers 1997, p. 27). From such estimations, it is blatantly obvious that electronic identification provides dramatic advantages and enhancements that traditional farming identification technologies can not provide.

The need to control disease outbreaks is obvious, and it is no surprise to see many of the authors describing the systems being put into place as being from Government departments. This aids to demonstrate the recognition within Government of the requirements and issues currently involved in RFID for livestock. Authors Rizoli (2003) and Nagl (2003) make an interesting point regarding terrorism, which is not something immediately obvious within livestock, however, upon consideration it appears entirely possible that such an attack could take place. Subsequently, their points regarding the requirement for RFID traceability programs so as to reduce the threat or impact of a terrorist attack appear quite valid.

4.2.3 Cost of implementing nationwide

Forster (2003) provides an estimate of how much it would cost to implement a whole-of-life electronic identification system in America. The cost of implementing such a system is estimated to range from $US2 to $US10 per head of cattle. Considering the 96 million head of cattle in America turning over a rate of approximately 35 million a year, top of the range chips are expected to cost about $US350 million per annum. Administering and maintaining the national database of information on each animal will provide a further cost, and understandably, debate over who will pay for such a system is quite intense. Considering such costs, it is likely that similar debates will be ongoing in many countries in the near future.

The figures quoted in this article are from 2003, and considering the trend of RFID costs to decrease over time, it can be considered that the costs for the present time will be less than the values specified in this article. The amount of cattle may also have changed, rendering the already wild estimate further unreliable. However the figures do provide a

good example of the large costs involved in implementing such an RFID system.

5 Australia's traceability system

The Australian dairy industry is valued at approximately $8 billion (Dairy Australia 2005). In 2004, this industry was composed of 9,611 registered dairy farms, hosting an estimated 2,028,000 dairy cows. Internationally, Australia ranks third in terms of world dairy trade (Dairy Australia 2004). Thus, it can be seen that the Australian dairy industry is certainly large and valuable.

5.1 The National Livestock Identification Scheme (NLIS)

In order to maintain trading relations with major customers and competitors (primarily the EU), Australia has developed its own individual whole-of-life traceability program for livestock – the National Livestock Identification Scheme (NLIS). This system is a "… permanent whole-of-life identification system that enables individual animals to be tracked from property of birth to slaughter for food safety, product integrity and market access purposes" (Meat and Livestock Australia n.d.a). Utilising RFID tags, this system is designed to record and communicate all movement of cattle from a property (whether it be from farm to farm or throughout the livestock chain) to the central NLIS national database. This system will not only ensure compliance with the EU trading standards (and likely any other countries who may develop similar standards for whole-of-life traceability in the future) (Meat and Livestock Australia n.d.a), but the NSW Department of Primary Industries – Agriculture (2004) states that,

> "Permanent identification will benefit the livestock industries by:
> - improving livestock traceability to reduce the impact of livestock disease and residue incidents;
> - making access to overseas markets more secure;
> - maintaining consumer confidence in Australian beef and dairy products;
> - offering producers improved herd management options; and
> - providing better proof of ownership to reduce stock theft."

5.2 Devices utilised in the NLIS

There are currently only two types of devices approved for use in the NLIS – a rumens bolus or ear tag utilising a low frequency RFID transponder. Both of these devices may be read while attached to the animal. No microchips (RFID devices placed under the animal's skin) have been approved for use in the NLIS as yet.

5.3 State control but national scheme

This system is coordinated at a state level, and has been compulsory in the state of Victoria since 2002 (Animal Health Australia n.d.), while New South Wales has enacted legislation to ensure state compliance with this system by the 1st of July 2005 (NSW Department of Primary Industries – Agriculture 2004), the same date that Queensland initiated the first of three phase-in stages (QLD Department of Primary Industries and Fisheries 2005). For the other states within Australia the system is currently only voluntary. However, the system will be implemented nationally in the near future, as all states/territories have agreed to progressively implement the NLIS (Victoria Department of Primary Industries – Agriculture and Food 2005).

5.4 New South Wales NLIS regulations

The following information pertaining to the NSW NLIS database (including approved NLIS devices and costs section) is drawn from the NSW Department of Primary Industries – Agriculture (2004) information website for the NLIS. Under the current NSW arrangements,

> - For the "phase in" year to 30 June 2005, cattle born from 1 July 2004 will have to be identified before they leave their property of birth.
> - From 1 July 2005, all cattle, irrespective of age, will have to be identified before they leave any property.
> - From 1 July 2005, saleyards will be required to notify the NLIS database of all cattle being sold. Abattoirs will be required to notify the database of all cattle slaughtered.
> - From 1 January 2006, all movements of cattle between properties must be notified to the NLIS database."

Once fully implemented, all cattle that leave a property for any reason

must be identified with an RFID tag and notification of the movement must be provided to the NLIS. Cattle that stay on their property of birth (as may happen for dairy cows) are not required to be identified, however the department states that the identification process may still be used if farmers wish to use the NLIS system for management purposes or to help with the recovery of cattle should they ever be stolen.

5.4.1 Moving cattle and who's responsible

When cattle leave the farm, even if on the way to an abattoir, they must be tagged and registered. From the 1st of July 2005, if cattle move to a saleyard or abattoir, it is up to the saleyard, agent, or abattoir to notify the NLIS of the movement of the cattle. From 1st of January 2006, if cattle move directly between properties for any purpose, it is the responsibility for the owner of person in charge of the cattle at the receiving property to notify the NLIS database of the movement.

5.4.2 Approved NLIS devices

To be approved for use in the NLIS, RFID devices must move through a process of examination and authorisation by a standards committee. This committee is charged with ensuring that proposed devices are of the correct electronic type, and meet national standards for quality and data retention. Approved NLIS devices are clearly identifiable as they feature the NLIS logo printed on them. It is an offence to use an unapproved RFID device, and also illegal to remove a functioning NLIS tag from an animal.

RFID identification devices (tags or boluses) are mandatory under the NSW NLIS scheme, however other available RFID components, such as readers, are not. Use of these additional components is left to the farmer's discretion.

5.4.3 Pricing and how to purchase the devices

Currently, all devices are available for purchase from Rural Lands Protection Board (RLPB) or from the farmer's rural merchant. The cost of an NLIS approved ear tag is approximately $3.50 per tag, while rumen boluses are slightly more expensive. There are no price estimates available for microchips as none have been approved to date.

The above information is provided by the NSW Department of Primary Industries – Agriculture (2004). As such, it is the most credible source of

information for the NSW NLIS, and provides a comprehensive wrap-up of the key issues and questions in implementing this system.

5.5 International recognition of the NLIS

RFID vendor Aleis International speak highly of Australia's NLIS, stating that "[t]he eyes of the world are firmly fixed on Australia as it continues to pioneer cutting-edge traceback and integrity management systems… It [the NLIS] is the largest and most sophisticated livestock database and management system currently in the world" (Aleis International n.d). Carrying such glowing statements through international markets will surely aid to promote Australia's ability for RFID adoption and disease-free animals throughout the world.

This glowing recommendation can be considered highly credible, as it would be expected that international RFID vendor Aleis International would be well aware of the various identification schemes adopted by various countries around the world. Being an Australian based company may pose a question of bias in their views however. Australian company Electro-com provide a degree of support for Aleis's statement, as they also state that the "Australian NLIS is the largest implementation of animal tracking in the world" (Electro-com 2004). This statement may also not be free of bias, however the two do back one another up, aiding to provide validity for the comments.

5.6 RFID standards

There are two main standards that are relevant to electronic animal identification. These have been defined by the International Organisation for Standardization (ISO):

- ISO 11784 – This international standard represents the structure of the radio frequency identification code for animals. This standard allows the bits communicated by the transponder to be interpretable by the transceiver (Geers et al. 1997, pp. 32-33; Eradus 2001, pp. 16-17).

- ISO 11785 – "This international standard describes the accepted protocol for transmission between the reader/scanner/interrogator and the transponder (tag)" (BeefStocker USA 2004). A central aim in the development of this standard is to facilitate communication with

transponders from a wide range of manufacturers with a common receiver (Finkenzeller 1999, p. 160).

As these are defined by the ISO, they are voluntary standards, and as such, there is no guarantee that vendors will elect to take up these standards if they feel that their own standard will achieve greater benefits for them. However, as consumer desires for compliance increase, and co-operation between vendors continues to grow (Anonymous 1999, p. 25), it can be seen that these standards are likely to play a dominant role in the future of RFID technologies.

Currently, a large number of vendors now design their readers and transponders to conform to these standards, aiding to remove incompatibilities between manufacturers. Such companies include the popular Texas Instruments (2004), and Allflex Australia (n.d.a) (who consider themselves the number one company in livestock identification). With such strong backing these standards look certain to have an impact and remain involved in the development of RFID devices for animal identification. They are also well documented, with three credible sources such as Geers et al. (1997), Finkenzeller (1999) and BeefStocker USA (2004) all featuring the standards. As the popularity of these standards grow, those vendors that elect not to comply risk being outcast from the market, as consumers will desire the device (tags and readers) that offer the most compliance with other devices (Anonymous 1999, p. 25; Ishmael 2003b, p. 16).

5.7 RFID temperature sensing (bio-thermo RFID)

“Temperature is the most important parameter to monitor in livestock” (Higgins 2003). Higgins (2003) interviews Digital Angel’s CEO Randolph Geisler, so as to gain an understanding of Digital Angel’s relatively new bio-thermo RFID microchip. These microchips are injected into the animal (under the skin), and provide temperature readings when interrogated by an RFID receiver/scanner. The article considers temperature fluctuations to be a great indicator of health problems in livestock.

Hostetter (2003) also interviews Geisler, and subsequently provides a similar view of the technology. The article notes that if any unusual temperature readings arise, then a farmer can be notified and take appropriate actions, such as removing this animal from the rest and

checking it for illness. Hostetter notes that Digital Angel is looking to advance this technology in the future, so as to possibly provide information on an animal's hormonal changes, blood pressure and even possibly disease identification. Conceding that most serious diseases may not be identifiable without extensive testing such as brain tissue, Hostetter notes that Geisler hypothesises that if someone can find a way to identify such diseases from another more measurable attribute of an animal then RFID may be the devices to perform this monitoring.

This bio-thermo technology provides a large range of benefits and possible uses. The ability to detect ill health before it progresses enough for visual signs to be evident is a highly useful device, and may be able to prevent the spread of illness through a group of livestock. These two articles are quite similar in their explanation and examples of the technology, however this is to be expected when they both interview the same person. Hostetter takes the discussion a little further however, and allows Geisler to reveal that they plan to provide further advances in livestock monitoring, which would be a great advance for RFID technology and livestock management on the whole.

6 Current RFID farm applications

The following are existing farm management practices that are deriving benefits from the use of electronic identification technologies. These applications provide examples of ways in which electronic identification can be used to exploit new opportunities, as stated by Geers (1997).

6.1 Reducing labour requirements

James (2004) provides an article describing direct benefits found by dairy farmers derived from the use of electronic identification. James states that ear tag recognition can be used to segregate cows as they pass through the milking parlour, reducing labour requirements on dairy units by up to £20, 000 per year. Providing a real life example of a milk producer, the article describes a farmer who fitted his cattle with an electronic ear tag costing £3 each. He utilises these tags to implement automatic segregation of cattle on their way to milking. As they head to milking, they pass through a race that contains gates to different areas,

one to the milking parlour and one to another paddock. As the cattle move through the race, their electronic identification devices are read. The gate to the milking parlour will open for those cows specified to be milked on the computer, while the gate leading to the other paddock will be the one to open for the rest. To perform such a task would have previously required the farmer to hire additional labour, however this is no longer required with the use of automatic identification devices, and the farmer may continue to expand his herd.

In another example from James, a farmer utilises automatic identification techniques so as to facilitate expanding his herd size from 280 to 450 cows. Automatic identification devices are estimated to cost the farmer an additional £6,000, however he estimates that it will reduce his labour bill by approximately £20,000 a year, thus providing an excellent cost-benefit ratio.

It can be seen from this article that electronic identification is providing real savings for dairy farmers. In these examples, the savings are being realized primarily due to a reduction of labour costs. This author has obviously targeted the article towards those in the dairy industry, as she uses terminology that is specific to this industry. It would have been beneficial if she explained these concepts and terminology, especially considering it may be read from others outside the industry due to the importance of the information being presented.

6.2 Controlled feeding

An article produced by ‘Yoke-L’ (n.d.) – a dairy cattle feeding system designed for operation inside a feeding parlour - describes the advantages that it offers for improved management of feed for the herd through electronic identification. The Yoke-L system can identify cows and provide individual cattle their specified rations, according to their lactation ‘calendar’. Many electronic identification systems can do this, however Yoke-L defines itself as being unique as it can mix forage and high protein additives. The feeding design features feed barriers with moving bail arms that provide access to the food. Mixed feed is spread along the trough or floor behind the feed barrier and supplements are added to this.

The farmer can vary the quality of the feed each stall, placing high

quality feed in some, and lower quality feed in others. This variation enables the high yielding cows to be given higher quality food whilst cheaper food can be given to those cows nearing the end of their lactation cycle, and producing less milk – obviously a more cost effective feeding system, while maximising the potential for milk production.

Yoke-L identifies and distinguishes between cows by electronic identification ear tags placed on each cow. As the cow approaches the feed barrier, the tag is electronically read, and the cow's identity number is compared with a database to derive her milk yielding value. A computer then

> "… decides whether she is entitled to the quality of feed at that position; if she is the bail arm opens and she can eat; if she is not, the bail arm stays closed and she wanders off to try her luck elsewhere" (Yoke-L n.d.).

Despite demonstrating cost savings through electronic identification, this article is somewhat misleading. The article initially identifies Yoke-L's ability to 'mix and match' ingredients as the key aspect that gives this feeding system its advantage over others. Similar language and writing style to this leads the reader to believe that Yoke-L is actually mixing the feed for each cow and providing it in the trough as per individual requirements or rules depending on the amount of milk the cows are yielding, readable from their RFID tags. However when the reader approaches the bottom of the article it becomes apparent that Yoke-L is not mixing the feed, but rather it is essentially mixing the cattle who are allowed access to the already varied feed. It is up to the cows themselves to find a feed barrier with food behind it that is of correct quality for their current needs, and not the other way around. Coupled with the cows changing lactation cycle (and thus varied milk production output), this may be a tricky concept for them to grasp, as they may be unable to identify a pattern in feeding arrangements. Additionally, information regarding how the feeding barriers are programmed to allow or deny cows entry would have been beneficial for this article. If such a system does work however, the cost benefits of saving high quality food could be significant for the farmer.

6.3 Improved milk yields and reduced operator stress through controlled feeding

Davies (1997) provides an example of how electronic identification has been used to provide measurable results in improved feed efficiency and increased milk yields. The article describes an electronic identification setup worth £9, 000 that was implemented in 1996 by large dairy RFID vendor Agricultural Technology Ltd. The system utilises individual passive RFID tags on each cow, combined with antennas at each stall within the feeding parlour. When a cow moves into a stall, these antennas interact with the tags to generate the required electromagnetic energy field, and a reader installed within the parlour receives the data. A unique piece of this design is that it utilises only one reader for the parlour, which can read data from up to 1000 antennas. The computer control unit for this system manages parlour feeding and milk yield records. Davies also states that the unit can store animal health information, and can be connected to a standard personal computer, thus enabling two way data exchange.

Under this system, cows enter the feeding parlour, and must enter the feeding stall directly beside the cow in front (which they apparently learn to do very quickly). Once they enter the stall, feed will only be released if the stall in front of them is occupied, and that occupant has been identified by the system and fed. Once this occurs, a predetermined amount of feed is automatically released to the newly identified cow. The farmer notes that the investment into electronic identification wasn't a luxury, but rather a necessity, so as to reduce his stress levels and provide improved feeding accuracy. He states that measurable benefits have been realised, as,

> "Before the change rolling average yield was 6500 litres a cow, of which 1932 litres came from forage. It is now 7300 litres, including 3000 from forage. Margins over purchased feeds have increased from £1300 a cow to £1438. Milk quality has also improved" (Davies 1997).

Obviously this demonstrates significant benefits gained from the usage of electronic identification. The farmer also claims he is much happier since the technologies introduction, and the cows are also more relaxed. However, he doesn't attribute all of these benefits to electronic

identification, as he states that his farm is trying hard to improve all areas of management, but this system certainly assists as at least know they know that the cows are receiving the right amount of feed every time.

It is certainly obvious from this article that significant gains were realised due to automating the feeding procedure through electronic identification. However, Davies leaves a lot of gaps in the article, and many assumptions have to be made to gain a comprehension of it. Davies doesn't provide any information regarding how the system determines what feed to be released, hence it is assumed that the user enters the amount of feed for certain cows into the computer controlling the RFID system. The specified amount of food and concentration is then provided to each cow depending on the individual specifications. The article also fails to identify the unit of measurement for the average amount of milk yielded from each cow. It is blatantly obvious that 6500 litres cannot be drawn from a cow in one milking session, leading to the assumption that the rate is measured per annum, however this is not confirmed anywhere in the article. Nor does the article explain the concept of the increased margins over purchased feed, or what has caused the rise in margins (other variables such fluctuating prices could achieve this). Mid-way through the article Davies also states that the system is capable of storing health information on the animals, however he doesn't define what health information this may be, or how it is derived and stored – perhaps manual entry or some automated process of detection and storage. The benefits identified look appealing, however a full comprehension of how these benefits are derived and their true significance cannot be achieved due to the brevity of this article.

6.4 Pig farm feed management

An article by Karnjanatwe (2005) explains a pig farm feeding system similar to those discussed above. Utilising electronic tags on individual pigs, automatic feeding stations are placed in the pen. When a pig approaches the feeding station through a one-way gate, an RFID reader will detect it and receive information from the tag. This will check the pigs ID, and gain it's characteristics including it's age and weight. The system will also determine if the pig has already eaten that day. If it is found to have already eaten, the gate to the feeding station will remain closed,

however if the pig has not yet eaten, the system will open the door to the feeding station and deliver the desired amount of food based on the pigs age and weight. When the pig has finished its food, an exit gate will open and the pig will exit. This technology is now a few years old however, and Karnjanatwe notes that maintenance costs are rising for the owners. As such, they are looking to update their RFID technologies.

Benefits of this system include increased efficiency as staff will know which pigs are fed and which are not, thereby reducing repeat consumption, while each pig has enough food for its needs. It was designed to subsequently reduce labour costs, while improving accuracy of the food quantity delivered to the pigs and to reduce food spillage that often occurred when food was distributed manually. This article provides a good description of this system, allowing the reader to gain a solid understanding of the systems operation. While the article is not directly related to dairy farms, the concepts of operation can be considered applicable to a dairy farm context.

6.5 Improved management options generating large savings

Three brothers who own a beef farm in the United States of America claim to have dramatically increased their profitability as a direct result of utilising RFID to track and manage cattle on an individual basis rather than groups. Ishmael (2001) reports that by using electronic identification tags to identify individual cattle, then sifting through the data using a specialised information system (AgInfoLink's 'Beeflink'), they believe they are saving between $US35-$US60 per head of cattle. "We're already using this to our advantage to make money. This isn't a theory; we've done it." States Tigh Cowan (one of the three brothers). They perceive the savings to be mainly related to the information they now have access to and can utilise to manage the farm. For example, they can get rid of poor performing cattle and keep the good ones, tell which paddocks have the most nutrition, evaluate mineral supplements in feed etc. These management capabilities, as well as possessing actual data relating to the cattle's life and development, have enabled the farmers to gain a higher than average price for their cattle at auctions. Treg Kusserz, another farmer utilising RFID states that "The more information you have, the better decisions you can make".

While Ishmael's (2001) article relates to the beef industry, it bears strong relation to the management operations of dairy farms also. It can be seen from this article that there is certainly money to be made from the use of electronic identification technology for improving farm management practices. However, this article simply provides the reader with an overview of the benefits these farmers are receiving. The article does not detail precisely what the farmers are looking for in the data, how they gain the data, what ways they use the data etc. This crucial information remains unrecorded.

7 Alternative approaches

Attempting to move beyond basic identification, Nagl et al. (2003) undertakes a project for the design of a remote health monitoring system for cattle. In this system, Nagl et al. attempt to use a range of sensors to constantly monitor cattle state of health, communicating biological information wirelessly to a base station through the use of Bluetooth technology. Nagl et al. identify the fact that at the time of writing, America had no mechanism in place to track animal identity in the fashion that Canada did, nor did they have any means to assess past or present animal health. The system they develop attempts to provide the ability for the livestock industry to react to and predict disease onset and spread, whether from natural or terrorist events.

Through the use of a GPS (Global Positioning System) unit to gather location and movement data, a pulse oximeter to measure blood oxygen saturation and pulse rate, a core body temperature sensor, an electrode belt to monitor pulse rate, a respiration transducer, and an ambient temperature transducer (Nagl et al. 2003, p. 3012), the project developed a wearable unit for cattle. This unit was designed to extract the biological information of the animal and communicate it to a base station via Bluetooth technology (which supports a ten metre read range) where it could then be analysed for any patterns that may indicate illness in the animal.

This project was obviously an investigatory undertaking, with numerous limitations in the unit developed. These included the size of the unit being quite large, and the battery life of various components of the

unit. Some interesting results were drawn however, and for most components, solid results were evident. Nagl et al. recognise the issues that arose, and state in their conclusion that there is a lot of research and development to be done on this topic, including the all-important ability to minimise the size of the wearable device and reduce power consumption to prolong battery life. The early prototype proposed by Nagl et al. is currently physically impractical and far too expensive for use, however the results of the project provide interesting prospects for cattle monitoring and tracking in future applications. Perhaps someday it may possibly integrate this project's device with RFID devices should the desire for this in-depth health monitoring arise.

It is immediately striking that the authors related their project to the need for animal identification in America, and noted the Canadian RFID tracking system. However, they did not utilise RFID for individual identification in their project, nor did they attempt to state why their system is preferable or what advantages it provides over the rapidly growing RFID system. They also alluded to the desire to track animal identities in the introduction (a specialist function of RFID technology), however failed to demonstrate how their system would provide this unique identification capability. Inclusion of RFID tags for individual identity tracking (at a minimum) appears quite possible however, and it would have been useful to see this integrated into this project. An alternative approach such as this does hold some intrigue and possibility for the future, however RFID remains the dominant technology of choice for providing individual cattle identification.

8 Conclusion

Despite the fact that RFID technology has been in existence for many decades, is only now maturing, and the time for mass adoption of RFID is nearing. Considering the worldwide trend towards whole-of-life identification and monitoring systems for livestock, it appears inevitable that RFID will have one of the biggest impacts on the livestock industries both in Australia and around the word. Considering the likely cost of implementing such a system ($3.50 per tag alone in NSW), it is important that farmers utilise this technology to derive additional benefits and return

on their investment through exploiting new opportunities for farm management.

References

Aarts, H.L.M., Langeveld, N. G., Lambooij, E. & Huiskes, J.H. 1992, Injectable transponders in pig production: applications and field trials. *Proceedings 12th International Pig Veterinary Society Congress*, The Hague, 17-20 August, p. 562.

Accenture. 2005, *RFID Tags as the New Product Code* [Online]. Available URL: http://www.accenture.com/xd/xd.asp?it=enweb&xd=services%5Ctechnology%5Cvision%5Csil_rfid_tags.xml [Accessed 18/3/2005].

Agri Signal. (n.d.), *Read Range and Read Probability Considerations Relating to Electronic Animal Identification* [Online]. Available URL: http://rapidttp.com/transponder/technote.html [Accessed 16/4/2005].

AIM Global. 2005. *Association for Automatic Identification and Mobility* [Online]. Available URL: http://www.aimglobal.org/ [Accessed 18/3/2005].

Aleis International. n.d., *National Livestock Identification Scheme* [Online]. Available URL: http://www.aleis.com/aleis/ai_natid_scheme.htm [Accessed 16/4/2005].

Allflex Australia. n.d.a, *ISO RFID Standards* [Online]. Available URL: http://www.allflex.com.au/31.html [Accessed 16/4/2005].

Ames, R. 1990, *Perspectives on Radio Frequency Identification*, Van Nostrand Reinhold, United States of America.

Animal Health Australia. n.d., *National Livestock Identification System (NLIS)* [Online]. Available URL: http://www.aahc.com.au/nlis/ [Accessed 19/3/2005].

Austin, R. 1995, 'Fine for beasts but what about staff?', *Farmer's Weekly*, 10 Feb., 45.

BeefStocker USA. 2004, *Glossary of electronic animal identification terms* [Online]. Available URL: http://www.beefstockerusa.org/rfid/glossary.htm [Accessed 16/4/2005].

Byteline Desk. 2005, *Radio Frequency Identification: Efficiency set to*

boost as RFID takes hold [Online]. Available URL: http://global.factiva.com.ezproxy.uow.edu.au:2048/en/arch/display.asp [Accessed 16/4/2005].

Canada ID. 2005, *CCIA Extends RFID Tagging Policy* [Online]. Available URL: http://www.canadaid.com/About/CCIAToExtendRFIDTaggingPolicy.pdf [Accessed 19/3/2005].

CCIA. 2005, *CCIA Extends RFID Tagging Policy* [Online]. Available URL: http://www.canadaid.com/About/CCIAToExtendRFIDTaggingPolicy.pdf [Accessed 19/3/2005].

Cochrane, T. Personal interview. 17 August 2005.

Corvallis Microtechnology. 2000, *Introduction to the Global Positioning System for GIS and TRAVERSE* [Online]. Available URL: http://www.cmtinc.com/gpsbook/chap8.html [Accessed 23/10/2005].

Dairy Australia. 2004, *Australian Dairy Industry in Focus 2004* [Online]. Available URL: http://www.dairyaustralia.com.au/template_default.asp?Page=Content/Markets_and_Trade/Australian_Dairy_Industry/index.htm [Accessed 22/10/2005].

Dairy Australia. 2005, *Dairying Areas of Australia* [Online]. Available URL: http://www.dairyaustralia.com.au/template_default.asp?Page=Content/For_Students/index.htm [Accessed 22/10/2005].

Davies, R. 1997, *Electronic Gains Aplenty* [Online]. Available URL: http://www.agricultural-technology.co.uk/fwedit/fwedit.html [Accessed 16/4/2005].

DeLaval. 2005a, *DeLaval Milking Point Controller MPC* [Online]. Available URL:http://www.delaval.com/Products/MilkingEquipment/Automation/Loose_housing/Milking_point_controller_MPC/default.htm [Accessed 22/10/2005].

DeLaval. 2005b, *Management of the Dairy Cow* [Online]. Available URL: http://www.delaval.com/Dairy_Knowledge/EfficientDairyHerdMgmt/Management_Of_The_Dairy_Cow.htm [Accessed 22/10/2005].

Finkenzeller, K. 1999, *RFID Handbook: Radio-Frequency Identification Fundamentals and Applications*, John Wiley & Son, Chippenham.

Food Production Daily. 2004, *Globalization of RFID boosts Advanced ID sales* [Online]. Available URL: http://www.foodproductiondaily.com/news/news-ng.asp?id=51979-globalisation-of-rfid [Accessed 19/3/2005].

Forster, J. 2003, 'Digital Angel soars on cattle worries' [Online], *Pioneer Press,* Dec 27. Available URL: http://twincities.com/mld/pioneerpress/business/7577278.html?template=contentM [Accessed 16/4/2005].

Frieden, D. J., Meyo, J. F., & Weston, W.C. 2002, Radio frequency identification tag formatting method [Online]. Available URL: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=6480100.WKU.&OS=PN/6480100&RS=PN/6480100 [Accessed 21/3/2005].

Geers, R., Puers, B., Goedseels, V. & Wouters, P. 1997, *Electronic Identification, Monitoring and Tracking of Animals*, CAB International, New York.

Gerdeman, J. D. 1995, *RF/ID: A Guide To Understanding And Using Radio Frequency Identification*, Research Triangle Consultants, North Carolina.

Gorman, G. E. & Clayton, P. 1997, *Qualitative Research for the Information Professional – A Practical Handbook*, Library Association Publishing, London.

Goth, G. 2005, *RFID: Not Quite Prime Time, But Dawdle at Your Own Risk*, *IEEE Distributed Systems Online* [Online], vol. 6, no. 2. Available URL: http://dsonline.computer.org/portal/site/dsonline/menuitem.6dd2a408dbe4a94be487e0606bcd45f3/index.jsp?&pName=dso_level1_article&TheCat=1025&path=dsonline/0502&file=o2003.xml& [Accessed 18/3/2005].

Hecht, B.K. & Hecht, F. 2004, *Radio ID Tags For US Drugs* [Online]. Available URL: http://www.medicinenet.com/script/main/art.asp?articlekey=40579 [Accessed 22/10/2005].

HerdLink. 2004, *NLIS* [Online]. Available URL: http://www.herdlink.com.au/nlis.shtml [Accessed 22/10/2005].

Higgins, K. T. 2003, *Engineering R&D: Temperature readings by remote*

control [Online]. Available URL: http://www.foodengineeringmag.com/CDA/ArticleInformation/features/BNP__Features__Item/ 0,6330,99353,00.html [Accessed 16/4/2005].

Hostettor, J. 2003, *Animal-tracking chips now let you in on how Fido is feeling* [Online]. Available URL: http://www.usatoday.com/tech/news/techinnovations/2003-04-21-animal-chip_x.htm [Accessed 16/4/2005].

ICF Consulting. 2004, *Automatic Identifiation: When to Use RFID* [Online]. Available URL http://www.icfconsulting.com/Publications/Perspectives-2004/IT-rfid.asp [Accessed 16/4/2005].

Ishmael, W. 2001, *The Power of One* [Online]. Available URL: http://beef-mag.com/mag/beef_power_one/ [Accessed 18/3/2005].

James, D. 2004, 'Automatic cow identification pays in the milking parlour'. *Farmer's Weekly*, p. 42.

Karnjanatwe, K. 2005, *How RFID tags can track livestock* [Online], Bangkok Post. Available URL: www.bangkokpost.com [Accessed 17/3/2005].

Meat and Livestock Australia. n.d.a, *About the NLIS* [Online]. Available URL: http://www. mla.com.au/content.cfm?sid=1350 [Accessed 18/3/2005].

Meat and Livestock Australia. n.d.b, *A Guide for Producers and Lot Feeders* [Online]. Available URL: http://www.mla.com.au/NR/rdonlyres/F0AC2D8A-27B4-4633-B823-AC4A6BC91B0D/0/PG_ Version30_Compiled.pdf [Accessed 22/10/2005].

Michael, K. 2003, *The technological trajectory of the automatic identification industry* [Online]. Available URL: http://www.library.uow.edu.au/adt-NWU/public/adt-NWU20040726.142447/ [Accessed 15 May 2006].

Morrison, M. J. & Curkendall, L. D. 2001**,** *Apparatus and method for reading radio frequency identification transponders used for livestock identification and data collection* [Online]. Available URL: http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/

netahtml/srchnum.htm&r=1&f=G&l=50&s1=6329920.WKU.&OS=PN/6329920&RS=PN/6329920 [Accessed 21/3/2005].

Nagl, L., Warren, S., Yao, J. & Schmitz, R. 2003, 'Wearable Sensor System for Wireless State-of-Health Determination in Cattle' [Online], *Engineering in Medicine and Biology Society - Proceedings of the 25th Annual International Conference of the IEEE*, Volume 4, pp. 3012 – 3015. Available URL: http://ieeexplore.ieee.org.ezproxy.uow.edu.au:2048/iel5/9009/28600/01280774.pdf?tp=&arnumber=1280774&isnumber=28600 [Accessed 16/4/2005].

New South Wales Department of Primary Industries – Agriculture. 2004, *National Livestock Identification System – questions and answers* [Online]. Available URL: http://www.agric.nsw.gov.au/reader/nlis/questions-answers-nlis-nsw.htm [Accessed 19/3/2005].

Ontario Ministry of Agriculture, Food and Rural Affairs. 1996, *Body Condition Scoring of Dairy Cattle* [Online]. Available URL: http://www.omafra.gov.on.ca/english/livestock/dairy/facts/92-122.htm [Accessed 22/10/2005].

Phillips, TAGSYS & Texas Instruments. 2004, *Item-Level Visibility in the Pharmaceutical Supply Chain: A comparison of HF and UHF Technologies* [Online]. Available URL: http://www.ti.com/rfid/docs/manuals/whtPapers/jointPharma.pdf [Accessed 16/4/2005].

Queensland Department of Primary Industries and Fisheries. 2005, *NLIS in Queensland* [Online]. Available URL: http://www.dpi.qld.gov.au/nlis/ [Accessed 22/10/2005].

RFID Journal. 2005a, *What is RFID?* [Online]. Available URL: http://www.rfidjournal.com/article/ articleview/1339/1/129/ [Accessed 18/3/2005].

RFID Journal. 2005b, *The Basics of RFID Technology* [Online]. Available URL: http://www. rfidjournal.com/article/articleview/1337/1/129/ [Accessed 18/3/2005].

RFID Journal. 2005c, *RFID Journal – The World's RFID Authority* [Online]. Available URL: http://www.rfidjournal.com [Accessed 18/3/2005].

RFID News. 2005, *Radio-Frequency Identification Devices* [Online]. Available URL: http://www.rfidnews.com/ [Accessed 18/3/2005].

RFID Times. 2005.*RFID Times* [Online]. Available URL:

http://rfidtimes.blogspot.com/ [Accessed 18/3/2005].

Rizoli. 2003, 'Where's the beef? Vt.'s Holstein Association tracks cattle with RFIDs in pilot program' [Online], *Mass High Tech*, Vol. 21, Iss. 9, p. 1. Available URL:http://proquest.umi.com.ezproxy.uow.edu.au:2048/pqdweb?index=0&did=303726401&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1113548978&clientId=20901 [Accessed 16/4/2005].

Semex. 2005, 'Morning, Noon and Night', *The Balance*, July, pp. 8-9.

Sensormatic. 1998, *Advantages of using RFID* [Online]. Available URL: www.sensormatic.com/smarteas. advantages.htm [Accessed 6/3/1999].

Sirit. n.d., *RFID* [Online]. Available URL: www.idsys.co.uk/english/intro_4.htm [Accessed 3/10/1997].

Texas Instruments. 2004, *Livestock ID* [Online]. Available URL: http://www.ti.com/tiris/docs/applications/ animal/livestock.shtml [Accessed 16/4/2005].

Victoria Department of Primary Industries – Agriculture and Food. 2005, *Your Guide to Victoria's Cattle Identification Legislation* [Online]. Available URL: http://www.dpi.vic.gov.au/dpi/nrenfa.nsf/9e58661e880ba9e44a256c640023eb2e/ca73fdb4fb0e9046ca256fd400159214/$FILE/_h9p64ikp0a4j42826clh20chg60qg_.pdf [Accessed 22/10/2005].

Want, R. 2004, 'The Magic of RFID' [Online], *Queue*, October. Available URL: http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=216 [Accessed 16/4/2005].

Williams, D. 2004, *RFID: Hot Technology with Wide-Ranging Applications* [Online]. Available URL: http://www.directionsmag.com/article.php?article_id=526&trv=1 [Accessed 19/3/2005].

Yoke-L. n.d., Yoke-L: The Bottom Line [Online]. Available URL: http://www.yokel.co.uk/bottom.htm [Accessed 16/4/2005].

7

Using scenario planning in the evaluation of information security applications

Laura Perusco

School of Information Technology and Computer Science, University of Wollongong

Abstract

This paper provides a broad overview of the scenario approach as it relates to the evaluation of location based services (LBS) technologies and their application. A scenario is a plausible vision of the future, based around a particular technology or application and developed via a scenario planning methodology. The main worth of the scenario planning approach is that it allows an application to be evaluated in terms of potential social impacts as well as technical merit and commercial viability. A sample scenario is presented within the paper to illustrate how the scenario planning methodology can be used. This scenario is analysed via deconstruction to draw out major issues presented regarding the use of LBS. The major contribution of this paper is a demonstration of the merits of scenarios in evaluating new technologies.

Keywords: scenarios, scenario planning, location-based services, evaluation methodology, social impacts

1 Introduction

This paper explains the use of scenarios and scenario planning methodologies as a tool in the evaluation and assessment of information security applications. It presents the specific example of a scenario that examines potential unintended effects of the widespread use of LBS.

In essence, a scenario is a narrative story. Though fictional, a good scenario is based on solid research and current technological capabilities. Developing a rich narrative around the potential uses of a technology creates a broad scope for exploring the social, ethical and legal implications of the technology. This paper looks at processes required to support the development and analysis of a cogent scenario, as well as the reasons for using scenarios when evaluating an information security system. A sample scenario is presented and analysed to illustrate the concepts described.

2 What is a scenario?

There is no single, authoritative definition of what a scenario is. The definition used in this paper is “[a]n internally consistent view of what the future might turn out to be” (Lindgren & Bandhold 2003, p. 21). A scenario is a narrative story that describes possible events in the future, however, to be plausible the events must be based on the past and emerge logically (Fazarkerley 2005, p. 79). Scenarios are designed to provide an overall picture of a possible future, and to describe this future in such a way that it is accessible to a layperson in the subject (Martino 2003, p. 722). Legal scenarios developed to demonstrate possible outcomes of a law (UTSCLC 2005, p. 3) are just one example of how scenarios are used by researchers. A major reason why a scenario approach is so useful to evaluating information security applications is that “new technologies cannot be analysed in isolation from their social context” (Weber 2002, p. 325).

Any credible scenario should aim to fulfil Godet’s (2000, p. 11) requirements that a scenario be relevant, coherent and plausible all at the same time, as well as being transparent. In the sample scenario presented here, footnotes are used extensively to help meet the requirement of transparency.

As well as conforming to Godet's constraints for plausibility, the scenario must be interesting. Fazakerley (2005, p. 79) cites various authors (including van der Heijden, Fahey and Randall, and Lindgren and Bandhold) as saying that no matter what scenario planning methodology is used, the story "must be memorable, interesting and rich in information whilst being creative". In this context, the researcher must endeavour to generate an original story based around the information security application being evaluated, creating interest through plot and character development while maintaining a rigid adherence to the requirements of plausibility, coherency and transparency.

2.1 Why use scenarios?

The Roman philosopher Seneca said: "[t]here is no favourable wind for the man who knows not where he is going" (Godet 2000, p. 3). Information security applications are often closely linked to people's lives, as is the case with LBS, yet the potential social effects of such applications are often ignored or sidelined. LBS is a perfect example of an area where social and legal analysis has been severely lacking and certainly not proportionate to the rapid pace of technological development.

With this in mind, there is certainly merit in exploring the potential effects of new security technologies and applications before they occur. "[T]oday's process of transition allows us to perceive what we are losing and what we are gaining; this perception will become impossible the moment we fully embrace and feel fully at home in the new technologies" (Žižek 1999, pp.101-102). Scenarios enable this kind of social analysis.

It is also important for analysis of possible future implications to keep pace with technological development. As Michael and Michael (2005, p.22) highlight:

> Most alarming is the rate of change in technological capabilities without a commensurate and involved response from an informed community on what these changes actually "mean" in real and applied terms, not only for the present but also for the future.

This statement emphasises the need for "soft" analysis tools such as scenarios in conjunction with business cases and profit models. Anyone who is concerned about the possible implications of information security

technologies should be able to access information about them. Potential issues involved with new commercially available technologies should be made available to a wide audience. Scenarios make complex issues readily accessible to citizens, making them comprehensible to the general public.

2.2 Limitations of scenario planning

The qualitative nature of scenario planning means that any scenario is unlikely to give a completely accurate prediction, but rather a plausible vision of how a particular information security application might affect society in the future. There are no concrete predictions or forecasts. However, at the same time, a quantitative methodology would not draw out the potential social and ethical issues from possible future uses of a technology.

In addition, the outcome of the scenario planning process is likely to be influenced by the scenario planning framework used. The one discussed here, TAIDA, is just one possible framework – there are others that may produce different results. Also, it is only viable to produce a limited number of scenarios, so countless others could conceivably exist.

Despite these limitations, scenarios can be exceedingly useful as a tool in the evaluation of information security applications. Perhaps the worth of scenario planning is best expressed by Godet (2000, p. 3):

> Unfortunately, there are no statistics for the future, and often personal judgement is the only information available to deal with the unknown. It is, therefore, necessary to gather other people's opinions before forming one's own, and then to place bets in the form of subjective probabilities.

3 The process of scenario planning

Although scenarios are a useful tool, their development requires a specific scenario planning framework to be effective. Many such frameworks exist. The scenario in this paper was created using the first three steps of TAIDA (Lindgren & Bandhold 2003, p. 38) to guide and structure the process. TAIDA actually involves five steps, and though the last two (deciding and acting) were beyond the scope of this paper, they

would certainly be useful in a practical evaluation.

According to Lindgren and Bandhold (2003), the first three steps of TAIDA are:

- *Tracking*: identifying aspects of the current situation and surroundings that may have an impact on the future under consideration (p. 47).
- *Analysing*: considering the possible future consequences of the aspects identified in the first stage (p. 39).
- *Imaging*: approaching possible changes intuitively to create a plausible future, “to create not only an intellectual understanding but also an emotional meaning” (p. 40).

Tracking has been performed by examining several existing precise LBS applications and reviewing literature pertaining to the possible future effects of LBS. The results of this process are largely presented within the actual scenario, with footnotes describing the bases for various aspects of the story. Analysing takes place in the background – the results of this step are not shown here other than as the grounding for the scenario. The results of the imaging step are presented as the scenario itself.

3.1 Scenarios as an evaluative tool

In light of the risk of attempting to evaluate information technology applications in isolation from social effects, scenarios become a very useful tool. The researcher can create a scenario depicting a plausible possible future where use of the application has become commonplace, using this vision to discuss potential societal impacts. A qualitative strategy such as this allows the complexities of the subject to be explored.

It is suggested here that scenario planning is one of three integrated approaches that may be used to explore the subject of possible social, ethical, legal and technological impacts of LBS. Although the data collection, scenario and analysis complement should one another, each serves a different purpose and thus requires a different method.

The primary focus for research is a qualitative content analysis of relevant articles about the technical capabilities of LBS and their possible future effects, with a scenario being developed based on this information through scenario planning. This is followed by a discussion of the legal, ethical, social and technological implications arising from the scenario, drawn out by deconstruction. Figure 1 shows the different methodologies

integrate to provide a solid analysis of potential future effects.

Figure 1: Relationship between methodologies used in developing and analysing a scenario

3.2 Analysing a scenario

It is proposed here that the most appropriate way to analyse a scenario is deconstruction. Deconstruction is an approach to literary analysis that aims "to create an interpretation of the setting or some feature of it to allow people … to have a deeper understanding" (Feldman 1995, p. 1). The object is to draw out the meaning of the text through interpretation (Hogan 1996, p. 9).

Deconstruction as an analytical tool is usually used to expose the ideological limits of the author by looking at what is said, what is omitted, and how dichotomies are used to present a particular viewpoint (Feldman 1995, p. 51). However, in the case of scenario analysis, these techniques may be used to look at the underlying issues presented through the narrative. Implementation consists of examining events in the scenario and considering the issues that underpin those events as well as why these issues arise.

4 Prisoners without prisons: a sample scenario

'Hey Janet. Sorry I'm late.' Scott slid into the other seat at the table.

Janet sighed, pushing a latte and a sandwich towards him. She'd already finished her coffee. She gestured to her PDA. 'These gadgets do everything. They compare our schedules, pick a place convenient to both of us, make sure there's something vegetarian on the menu for me, and book a table.[3] Pity they can't get you here on time too.'

[3] This is similar to one of the scenarios that Lin, Yu and Shih use to illustrate the uses of pervasive commerce (p-commerce). One of their scenarios involves two people, John and Nancy, at different stores in a mall wanting to meet up for lunch. Their intelligent devices identify their locations and when they are

‘I’m sure it’s on the horizon,’ Scott joked. ‘So how’s life in the Sydney office?’

‘All right. The weather makes a nice change – I’m starting to get used to seeing sunshine in spring. How about your parolees?’

Scott laughed. ‘There’s a lot more of them. In Melbourne I had fifty or sixty cases at once. Now I’ve been allocated more than a hundred.’ He bit into his sandwich. ‘With less parole officers able to handle more cases, I guess I’m lucky to have a job,’[4] he continued with his mouth full.

Janet raised her eyebrows. ‘With a lot of women intolerant of bad table manners, you’re lucky to have a girlfriend. I assume the workloads are greater because they use those chips here?’

‘The *caseload* is greater, the workload is the same – yeah, because of the chips.’[5] He smiled. ‘It’s crazy that NSW is already trialling these tracking implants,[6] while Victoria’s only recently got a widespread implementation of the anklets. They’ve been around for years.

‘The implants are much better,’ Scott continued. ‘Who wants a chunky anklet or bracelet that makes you look like collared freak? I’ll bet it’s really disconcerting having people stare at you suspiciously in the street,

likely to be ready, and present a list of nearby restaurants that could be reserved for lunch in 20 minutes [Lin, Lu and Shih 2005, p. 166]. This idea has been extended here to filtering restaurants by available menu selections.

[4] There is strong competition for available parole officer positions with the Department of Corrective Services in NSW (Department of Education, Science and Training 2005).

[5] Electronic monitoring may allow parole officers to take on more cases than was previously possible because some of their normal duties can be automated. However, it must be remembered that technology is merely a tool – electronic monitoring is not a substitute for parole officers (American Probation and Parole Association 1996).

[6] The “tracking implants” referred to here are subdermal GPS-enabled personal locators – implantable GPS tracking devices. Although such technology is not currently available, it may not be far off. Applied Digital Solutions (the same company that developed the VeriChip) has announced a working prototype of this type of device. The prototype is quite large – about 5cm long and 1cm deep – but the company expects to be able to miniaturise the implant to the point where it is about the size of a grain of rice (Applied Digital Solutions 2003).

knowing that you're a criminal. It kind of defeats the purpose of parole – the idea is rehabilitation, reintegration under supervision. That's why the implants are so good – there's no stigma attached. No one can even tell you have one. And they're harder to remove, too.'

'I don't see what the big deal is,' Janet replied. 'Why not just keep people under lock and key?'

'Resources. It costs a lot to keep someone imprisoned, but the cost drops significantly if you imprison them in their own home instead.[7] It's about overcrowding, too – jails everywhere have had an overcrowding problem for years.[8]

'I also think electronic monitoring and parole are much better in terms of rehabilitation,' Scott went on. 'People can change.[9] Often they've committed a fairly minor crime,[10] then they go to prison, get mixed up with worse crowds. It can be pretty rough in there. There is certainly a danger that by imprisoning people with "harder" criminals, you run the risk of corrupting them further and exacerbating the problem.[11]

[7] One NSW report stated that the daily cost of full-time imprisonment for one person was around $177 in maximum security, compared to $30 for home detention (NSWLRC 1996, p. 17). Using home detention rather than imprisonment equates to a saving per offender of $53,655 each year.

[8] "Overcrowding is endemic to the Australian prison system … Despite [a] significant number of new prisons built in the 1990s most Australian prison systems were operating above optimal capacity in 1998-99 and some like WA, SA and Qld were well above capacity" (Brown et al 2001, p. 1468).

[9] "Parole is rooted in the fundamental belief that offenders can be motivated to make positive changes in their lives" (American Probation and Parole Association 2002).

[10] A study of a two-year electronic monitoring trial program for parolees in the U.K. found that 89 percent of low-to-medium risk parolees completed their parole successfully. This was compared with 82 percent for medium-to-high risk parolees and 75 percent for high risk (Sugg, Moore and Howard 2001). When parole was first introduced to Australia in 1966, the element of risk inherent in such a system was recognised by the legislature. However, this was balanced against the same risks which are present when an offender is released into the community, unsupervised, at the end of his or her sentence. Parole seeks to limit community risk by promoting rehabilitation (Law Reform Commission NSW 1996).

[11] Jails are often places where inmates learn more about crime than socially acceptable behaviour. Some prisoners are also vulnerable to brutalisation from other prisoners or even from prison officials. This can produce an embittered person who, upon release, goes on to commit far worse crimes than those for which they were originally incarcerated (Brown et al 2001, p. 1469).

‘On parole, they can still go to work and earn money, be productive members of society, get their lives back.[12] But they’re watched, very closely – the tracking systems alert us if anything looks off. It’s imprisonment without prisons.’

Janet gave him a sceptical look. ‘So you’re turfing people out of jails? How do you determine who gets paroled and who doesn’t?’

‘Well, a while ago it was mainly based on crime-related and demographic variables,’ Scott replied. We’re talking stuff like what sort of offence they’re doing time for, the types of past convictions on their record, age, risk of reoffending.’[13]

Janet nodded.

‘Now a bunch of other things are looked at too,’ he continued, finishing off his sandwich. ‘It’s a lot more complex. Psychological factors play a big part. Even if someone displays fairly antisocial traits, they’re still considered pretty low risk as long as they don’t also show signs of mental illness.’[14]

‘What about terrorists?’ Janet argued. ‘How can you guarantee that there won’t be an incident in Australia like the London rail bombings?’

[12] Ostensibly, the main rationale for parole is the community benefit that stems from the rehabilitative effects of supervised, conditional early release. However, it seems apparent that at least part of the reason for parole is economic – the costs to the government and community of imprisonment are fairly obvious [Law Reform Commission NSW, above n 187]. One of the most significant advantages of parole and home imprisonment is that they allow the offender to work and pay taxes (and possibly even pay for their own monitoring costs), reducing the burden on the rest of society (National Law Enforcement and Corrections Technology Center 1999).

[13] When considering whether or not to make a parole order, the NSW Parole Board is bound to consider a number of matters under s135(2) of the *Crimes (Administration of Sentences) Act 1999*. These issues include the offender’s previous convictions, the offender’s conduct in serving his or her sentence so far, and the likelihood that the offender will be able to adapt to normal community life. The Board must also consider reports prepared by or on behalf of the Crown in relation to the granting of parole (New South Wales Council for Civil Liberties 2003). It is assumed that such reports may take additional factors into account besides those listed in the *Crimes (Administration of Sentences) Act 1999*.

[14] This idea comes from a paper about predictive models of inmate misbehaviour in institutions, but has been extrapolated to misbehaviour on parole (Lee and Edens 2005, pp. 412-414).

‘Like I said, anyone considered really dangerous is still kept in a regular prison,’ Scott said. ‘And we’d be able to tell by location monitoring if a parolee was doing anything suspicious. There’s no way a convicted terrorist would get anywhere near anything worth attacking.

‘And you know that governmental powers now allow “persons of interest” to be implanted as well.[15] No one even remotely suspicious would be able to target a major landmark, business or tourist centre without alarm bells going off all over the place.’

Janet shook her head. ‘I’m all for preventing terrorist attacks. But implanting people who haven’t committed a crime? How far will they take it? What if the government decided that we should just track everyone, to be on the safe side?’

Scott shrugged. ‘I guess we just need to find a nice balance between personal freedom and national security.’

He glanced at his watch and pushed his chair back. ‘I need to get back to work,’ he said apologetically.

5 Analysing the scenario

An analysis of the scenario above, *Prisoners Without Prisons*, reveals a number of important issues related to the use of LBS in enhancing national security. These include the ethical dilemma of using LBS to track suspected criminals, how LBS fit into society, and the momentum of LBS technologies. This section demonstrates how analysis of a scenario can be used to draw out such issues.

5.1 The ethics of pre-emptive control

Perhaps the most significant dilemma presented in *Prisoners Without*

[15] Australia’s new anti-terrorism laws, among other things, allow people reasonably suspected of being involved in terrorism to be tracked and monitored for up to 12 months (Gilmore 2005). In a rather prophetic statement, Michael and Michael (2005, p. 25) state in their ‘Microchipping People’ article: “[i]f terrorism attacks continue to increase in frequency, there is a growing prospect of the use of chip implants for identification purposes and GPS for outdoor tracking and monitoring.”

Prisons is the use of LBS technologies to monitor people such as those suspected of being involved in terrorist activities. As mentioned in the footnotes, this is not mere fancy – the Australian Government has enacted new anti-terrorism laws that, among other things, give police and security agencies the power to fit terror suspects with tracking devices for up to 12 months (Gilmore 2005).

This kind of power should give rise to concern. Can it be considered reasonable to impinge upon the freedom of someone who is merely suspected of committing a crime? For tracking implants especially, do governments have the right invade a personal space (i.e. a person's body) simply based on premise?

Criminals give up some of their normal rights by committing an offence. By going against society's laws, freedoms such as the right to liberty are forfeited. This is retributivism (i.e. "just deserts"). The central idea is proportionality: "punishment should be proportionate to the gravity of, and culpability involved in, the offence" (Brown et al 2001, p. 1376). With no crime involved, the punishment of electronic monitoring or home detention must be out of proportion.

This researcher does not make a judgement on whether pre-emptive control legislation is good or bad. It is suggested, however, that the laws recently proposed by the Federal Government (and agreed to by the States) could be indicative of a broader trend. Prime Minister John Howard said that "[i]n other circumstances I would never have sought these new powers. But we live in very dangerous and different and threatening circumstances … I think all of these powers are needed" (Kerr 2005, p. 1). Could the same argument be used in the future to justify monitoring everyone in the country? Everyone's privacy being invaded in such a way would likely lower significantly the chance of crimes being committed, or at least the chance of criminals remaining unpunished. If pre-emptive control is a part of government security, then widespread LBS monitoring could be the most effective form of implementation.

Without suggesting a far-fetched Orwellian scenario where draconian policies and laws mean that the entire population is tracked every moment of their lives, there is a possibility that the current climate is indicative of individuals' willingness to relinquish their privacy (or at least someone else's) for the sake of enhanced security.

5.2 The neutrality (or otherwise) of LBS technologies

There is a widely held belief that it is how people use a technology, not the technology itself, that can be characterised as either good or bad. People often see technology as neutral "in the sense that in itself it does not incorporate or imply any political or social values" (Lipscombe and Williams 1979, p. 19). The converse argument is that technology is not neutral because it requires the application of innovation and industry to some aspect of our lives that "needs" to be improved, and therefore must always have some social effect.

The uses of LBS presented in the scenario suggest that the technology itself is not neutral – that LBS are designed to exercise control. This may be control over one's own situation as presented at the beginning of the scenario, where Janet and Scott meet for lunch. Alternatively, it may be forced control over parolees and other criminals or suspected criminals. These situations imply that LBS is not neutral, and that the technology is designed to enhance control in various forms.

5.3 The technological momentum of LBS

Some believe that technology is the driving force that shapes the way we live. This theory is known as technological determinism, one of the basic tenets of which is that "changes in technology are the single most important source of change in society" (Winner 1977, p. 76). The idea is that technological forces contribute more to social change than even political, economic or environmental factors.

This researcher would not go so far as to subscribe to this strongest sense of technological determinism doctrine. The social setting in which the technology emerges is at least as important as the technology itself in determining how society is affected. As Braun says: "[t]he successful artefacts of technology are chosen by a social selection environment, [like] the success of living organisms is determined by a biological selection environment" (Braun 1995, p. 21). Technologies that fail to find a market never have a chance to change society, so society shapes technology at least as much as it is shaped by technology. In this light, Hughes's theory of technological momentum is a useful alternative to technological determinism: similar in that it is time-dependent and focuses on

technology as a force of change, but sensitive to the complexities of society and culture (Hughes 1994, 101).

Technological potential is not necessarily social destiny. However, in the case of LBS, it is plausible to expect it to create a shift in the way we live. We can already see this shift occurring in parents who monitor their children with LBS tracking devices, and in the easing of overcrowding in prisons through home imprisonment and parole programs using LBS monitoring.

As described previously, the threat of terrorist attacks has led the Australian Government to give itself extraordinary powers that never could have been justified previously. In this situation, LBS has enabled the electronic monitoring of suspicious persons, however, it is not the technology alone that acts as the impetus. Pre-emptive electronic tracking could not be put in place without LBS. Neither would it be tolerated without society believing that it is necessary in the current climate of unrest.

The scenario also demonstrates that technology and society evolve at least partially in tandem. Through the conversation between Scott and Janet, we learn that LBS tracking implants were not introduced simply because they were technically feasible. The reasons for their use were to reduce overcrowding in prisons and to mitigate the burden of criminals on the ordinary taxpayer. Social and economic factors, as well as technological ones, contributed to this measure being taken.

Although technology is not the sole factor in social change, and arguably not the most important, LBS are gaining momentum and are likely to contribute to a shift in the way we live. This can be seen both in the scenario and in real-life examples today.

6 Conclusion

This paper has presented an overview of scenarios as an evaluative tool. Although scenario planning has its limitations, it should certainly not be ignored entirely. It is important to consider social issues as well as technical problems when assessing an information security application. Scenario planning provides a framework for exploration. Although any particular scenario *per se* is unlikely to come true, it provides an example

of what *could* happen if the technology is in widespread use, and gives ground for prevention or mitigation of potential undesirable effects. The scenario presented here illustrates how the technique can generate a plausible vision of how technologies may affect a particular situation. It must be kept in mind that a technology cannot be evaluated in isolation from its impact on society, and it has been demonstrated here that scenarios can be a very useful tool for analysis of such issues involved in a technology's application.

References

Applied Digital Solutions, *Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device* (2003) <http://adsx.com/news/2003/051303.html> [Accessed September 21, 2005].

American Probation and Parole Association, *Discretionary Parole* (2002) <http://www.appa - net.org/ about%20appa/discretionary_parole.htm> [Accessed September 25, 2005].

Braun, E., *Futile Progress: Technology's Empty Promise* (1995).

Brown, D., Farrier, D., Egger, S. and McNamara, L., *Criminal Laws* (3rd ed, 2001).

Department of Education, Science and Training, 'Probation Officer/Parole Officer – NSW/ACT', *Job Guide 2005* (2005) <http://jobguide.thegoodguides.com.au/statespecific.cfm?jobid=615 &state_id= NSW> [Accessed September 24, 2005].

Fazakerley, V., *Critical Issues for the Future of the Australian Urban Water Supply Industry*, PhD thesis, Curtin University of Technology (2005).

Feldman, M.S., *Strategies for Interpreting Qualitative Data* (1995).

Gilmore, N., 'PM defends anti-terrorism laws', *Lateline* (September 8, 2005) <http://www.abc.net.au/ lateline/content/2005/s1456384.htm> [Accessed September 22, 2005].

Godet, M., 'The Art of Scenarios and Strategic Planning: Tools and Pitfalls', *Technological Forecasting and Social Change*, (Sep 2000) Vol. 65, Iss. 1, 3.

Hogan, P., *On Interpretation: Meaning and Inference in Law, Psychoanalysis, and Literature* (1996).

Hughes, T.P., 'Technological Momentum' in Smith, M.R. and Marx, L. (eds), *Does Technology Drive History?* (1994) 101.

Kerr, J., 'House arrest for terror suspects', *The Sydney Morning Herald* (September 28, 2005) 1.

Law Reform Commission NSW, 'Chapter 7: Parole' *Discussion Paper 33(1996) – Sentencing* (1996) <http://www.lawlink.nsw.gov.au/lrc.nsf/pages/DP33CHP7> [Accessed September 25, 2005].

Lee, S.J. and Edens, J.F., 'Exploring Predictors of Institutional Misbehavior among Male Korean Inmates', *Criminal Justice and Behaviour* (Aug. 2005) Vol. 32, No. 4, 412.

Lin, K.J., Yu, T. and Shih, C.Y., 'The Design of A Personal and Intelligent Pervasive-Commerce System Architecture', *Proceedings of the Second IEEE International Workshop on Mobile Commerce and Services* (2005).

Lindgren, M. and Bandhold, H., *Scenario Planning: The link between future and strategy* (2003).

Lipscombe, J. and Williams, B., *Are Science and Technology Neutral?* (1979).

Martino, J.P., 'A review of selected recent advances in technological forecasting', *Technological Forecasting and Social Change* (Oct 2003) Vol. 70, Iss. 8, 719.

Michael, K. and Michael, M.G., 'Microchipping People: The Rise of the Electrophorus', *Quadrant* (Mar 2005) Vol. 49, Iss. 3, 22.

National Law Enforcement and Corrections Technology Center, 'Keeping Track of Electronic Monitoring', *National Law Enforcement and Corrections Technology Center Bulletin* (Oct. 1999) <http://www.justnet.org/pdffiles/Elec-Monit.pdf> Accessed September 25, 2005].

New South Wales Council for Civil Liberties, *Parole, Sex Offenders and Rehabilitation Programs* (Feb. 2003) <http://www.nswccl.org.au/docs/pdf/Parole_SexOffenders_Note.pdf > [Accessed September 25, 2005].

NSWLRC, *NSWLRC Report 79: Sentencing* (1996).

Sugg, D., Moore, L. and Howard, P., 'Electronic monitoring and offending behaviour: reconviction results for the second year of trials of curfew orders' (2001) <http://www.probation.homeoffice.gov.uk/files/pdf/r141[1].pdf> [Accessed September 24, 2005].

UTSCLC, *Be Informed: ASIO and Anti-Terrorism Laws* (February 2005) 3.

Weber, K.M., 'The Political Control of Large Socio-technical Systems: New Concepts and Empirical Applications from a Multidisciplinary Perspective' in Sørensen, K.H. and Williams, R. (eds) *Shaping Technology, Guiding Policy: Concepts, Spaces and Tools* (2002) 325.

Winner, L., *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (1977).

Žižek, S., 'Cyberspace, or the Unbearable Closure of Being' in Janet Bergstrom (ed), Endless Night: Cinema and Psychoanalysis, Parallel Histories (1999) 92.

8

Regulating telecommunications interception & access: a seachange in surveillance laws

Simon Bronitt and James Stellios

ANU College of Law, The Australian National University

Abstract

The federal Parliament's recent amendments to the telecommunications interception legislation have significantly overhauled the regulatory scheme for the protection of communications passing over the telecommunications system. The amendments have introduced new provisions for accessing stored communications, and have provided government agencies with further tools for security and law enforcement purposes. This paper considers the changes to the legislative scheme, and how privacy interests have been 'balanced' away in favour of providing government agencies with enhanced surveillance tools.

Keywords: privacy, telecommunications interception, surveillance, data access, wire tap, warrants, security, law enforcement

1 Introduction

The federal Parliament has recently amended the legislative scheme for the regulation of telecommunications interception, representing possibly the most significant overhaul and expansion since the current regime was established by the *Telecommunication (Interception) Act 1979* (Cth) ('The TI Act'). The changes were introduced to implement recommendations of a 2005 review by Anthony Blunn ('the Blunn Report').[16]

Prior to the 2006 amendments, the TI Act regulated the interception of communications passing over a telecommunications system, prescribing general prohibitions on interception and subsequent use of intercepted communications, and a range of exceptions. While the original intention of the legislation may have been to protect national telecommunications infrastructure, the prevailing view is that the legislation is an important vehicle for the protection of privacy for those using the telecommunications system. This conception of the purpose of the prohibitions in the TI Act creates a tension with the purpose underlying the important exceptions: primarily the warrant system for security and law enforcement purposes. Accordingly, reforms which have expanded the legislative scheme have been seen as requiring the 'balancing' of interests in privacy protection with the interests in security and law

[16] Anthony Blunn, *Report of the Review of the Regulation of Access to Communications* (2005).

enforcement.

This 'balancing' approach was put to the test with the 2006 amendments to the TI Act. The TI Act, renamed the *Telecommunication (Interception and Access) Act 1979* (Cth) ('TIA Act'), was amended to expand the regulatory scheme to cover prohibitions on access to stored communication (i.e., put broadly, communications that have ceased passing over the telecommunications system) and subsequent use, and exceptions to those prohibitions. While these exceptions are structurally similar to those under the interception provisions, the scope of those exceptions is much broader. The new TIA Act also expands the interception tools for security and law enforcement, with the introduction of device warrants and B-Party warrants (i.e., those directed to innocent third parties because of their connection with a 'person of interest').

The amendments were introduced by the government into the House of Representatives on 16 February 2006, and passed the Senate on 30 March 2006. After their introduction into the Senate on 1 March, the amendments were referred to the Senate Legal and Constitutional Legislation Committee ('the Senate Committee'), which reported on 27 March. The Senate Committee produced a report, with the bipartisan support of government and opposition members, which expressed concerns that many of the amendments impacted unduly on privacy interests, and recommended a range of amendments. The Democrats produced a supplementary report, which dissented only to the extent that it recommended further changes to protect privacy. The Senate Committee, it seems, came to the view that the new amendments got the 'balance' wrong. However, its recommendations designed to restore the 'balance', for the most part, were not accepted by the government. The amendments were passed by a government controlled Senate, with the commitment that the government would continue to consider the Senate Committee's recommendations.

This paper will consider, first, how the 2006 amendments have affected the interception provisions in the TIA Act (Part 2) and, secondly, the new stored communications scheme introduced by the amendments (Part 3). In the final part (Part 4), the paper will argue that the process of law reform,

as well as the provisions of the TIA Act, demonstrate how privacy interests have been 'balanced' away in favour of providing government agencies with surveillance tools for the purposes of national security and law enforcement.

2 Interception Regime

2.1 Introduction

The core provisions relating to the interception of telecommunications have remained in place following the 2006 amendments. This section will explain the legislative scheme under the TI Act for interception, and how the 2006 amendments have affected the provisions. Telecommunications interception in Australia has been regulated exclusively at the federal level since 1960 with the enactment of the *Telephonic Communications (Interception) Act 1960* (Cth). Under the *Constitution,* the federal Parliament has legislative power to enact laws with respect to 'postal, telegraphic, telephonic and other like services'.[17] Although this power is concurrent with the legislative power of State Parliaments, the High Court has held that the exhaustive federal legislation in the area leaves no room for State intervention.[18]

The TI Act was enacted to replace the *Telephonic Communications (Interception) Act 1960* (Cth). The long title of the TI Act described the legislation as 'An Act to prohibit the interception of telecommunications except where authorised *in special circumstances* or for the purpose of tracing the location of callers in emergencies, and for related purposes.' The matters motivating the enactment of the TI Act included *security matters and the detection of narcotic offences*.[19] It is quite clear, however,

[17] *Commonwealth Constitution*, s 51(v). The constitutional validity of the legislation has been upheld in various cases: *Grollo v Commissioner of Australian Federal Police* (1995) 184 CLR 348; *Love v Attorney-General (NSW)* (1990) 169 CLR 307; *Hilton v Wells* (1985) 157 CLR 57; *John Fairfax Publications Pty Ltd v Doe* (1995) 37 NSWLR 81; *Kizon v Palmer* (1997) 72 FCR 409.

[18] *Miller v Miller* (1978) 141 CLR 269.

[19] Second Reading Speech, Telecommunications (Interception) Bill, House of Representatives, 23 August 1979, 560.

that the scope of the legislative scheme has shifted considerably from its original intentions.

2.2 The interception provisions – prohibition on interception

The interception prohibitions in the TIA Act work in two phases. The first, considered in this section, is the prohibition on interception. The second, considered in Part 2.6, is the prohibition on subsequent use of intercepted communications. Subject to a range of exceptions, the TIA Act prohibits the interception of communication passing over a telecommunications system (s 7(1)). 'Communication' is defined in s 5(1) to include a 'conversation and a message', in whole or part, whether in the form of: speech, music or other sounds; data; text; visual images; signals; or in any other form or in any combination of forms. An 'interception of a communication passing over a telecommunications system' consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (s 6(1)). The 2006 amendments seek to provide clearer guidance as to when a communication is passing over a telecommunications system. A communication starts passing over a system when it is sent or transmitted by the sender, and continues passing over the system until it becomes accessible to the intended recipient (s 5F). A communication 'is accessible to its intended recipient if it has been received by the telecommunications service provided to the intended recipient, is under the control of the intended recipient, or has been delivered to the communications service provided to the intended recipient' (s 5H).

The Act excludes from these definitions communications to emergency services numbers (s 6(2B). Until the 2006 amendments, there was another important exception for interceptions by persons lawfully on premises listening to communications (s 6(2)). When the TI Act was first enacted, the exception in s 6(2) was intended to exempt the activities of telecommunications carriers and their employees from the prohibition on interception to allow equipment testing. The Explanatory Memorandum to the 2006 amendment stated that the operation of the provision 'has

become redundant in the deregulated and rapidly changing telecommunications environment',[20] and its continued operation only 'undermines the strict privacy protections contained in the Act because it may allow participant monitoring.'[21] During the Senate Committee inquiry, submissions were made opposing the repeal of the provision on the basis that it had other useful applications, including allowing organisations to monitor incoming email for viruses and to filter spam.[22] The Senate Committee supported the repeal of the provision on the basis that other amending provisions would address the concerns expressed.[23]

2.3 The exceptions to the prohibition on interception – the warrant system

The TIA Act (Parts 2.2, 2.3, 2.5) sets out a number of exceptions to the prohibition on interception, principally interceptions pursuant to a warrant. There are two types of warrants: Part 2.2 warrants and Part 2.5 warrants. Part 2.2 warrants may be issued to the Australian Security Intelligence Organisation ('ASIO') by the federal Attorney-General and the Director-General of Security for intelligence gathering in relation to national security or for the purpose of obtaining foreign intelligence.

Part 2.5 warrants may be issued by federal judges and members of the Administrative Appeals Tribunal ('AAT') to federal[24] and State law enforcement agencies to intercept telecommunications made in connection with the investigation of specified federal and state offences.

[20] Explanatory Memorandum, Telecommuncations (Interception) Bill 2006 (Cth) 48.

[21] Ibid.

[22] Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 14 March 2006 (The Australian Banker's Association); Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 20 March 2006 (Telstra).

[23] Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Bill 2006* (2006) paras 5.23-5.24. Specifically, the Committee was of the view that the new s 108(2) would address the concern. Subsection 108(2)(e) provides an exception to the prohibition on accessing stored communication for a person exercising duties relating to the installation, connection or maintenance of equipment.

[24] Federal law enforcement agencies are the Australian Federal Police and the Australian Crimes Commission: see definition of 'Commonwealth agency' in s 5.

Thus, although the scheme is federal, the legislation does not limit Part 2.5 warrants to federal law enforcement officers. In fact, the latest Annual Report by the Attorney-General to Parliament on the operation of the TI Act for the year ending 30 June 2004 reveals that two-thirds of Part 2.5 warrants were issued to State rather than federal agencies in the last three reporting years (see Table 1).[25] State agencies may apply for Part 2.5 warrants where they have been declared to be eligible by the federal Attorney-General.[26] A declaration can only be made where the federal Attorney-General is satisfied that the States have enacted legislation requiring the State authorities to meet inspection and reporting requirements equivalent to those set out for Commonwealth agencies.

The scope of the warrant exception has expanded significantly from its original operation. Prior to the TI Act, the *Telephonic Communications (Interception) Act 1960* (Cth) permitted only limited exceptions to the prohibition on the interception of telephonic communications, including circumstances where a warrant had been granted by the federal Attorney-General or Director-General of Security for national security purposes. The enactment of the TI Act saw the scheme expanded to allow the issue of warrants for narcotic offences to advance the federal government's 'war on drugs'. Since the late 1980s, the TI Act has been broadened to include categories of offences beyond drugs, most recently to terrorism offences.

Prior to the 2006 amendments, the categories of offences were divided into serious 'Class 1 offences' which included murder, kidnapping, narcotic and terrorism offences. Lesser offences were designated 'Class 2 offences', which included offences involving loss of life or serious injury, serious property damage, serious arson and child pornography. Under this twofold classification privacy considerations were restricted to 'Class 1' offences only. As we shall explore below in 2.5, the utility and practical effect of this approach (in terms of establishing a more stringent threshold for granting Class 1 warrants) is contestable. Indeed, 2006 amendments have removed the distinction between Class 1 and Class 2 offences,

[25] The report for the year ending 30 June 2005 has not yet been reported to Parliament.

[26] The definition of 'eligible authority' in s 5 of a State covers State police forces and other listed State crime and corruption agencies.

redefining existing offences under Classes 1 and 2 offences as 'serious offences' and applying privacy as a factor to be considered in *all* cases. These amendments were supported by the Senate Committee.[27]

Table 1 – Applications for Part 2.5 Warrants (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004,* Table 1).

AGENCY	RELEVANT STATISTICS	APPLICATIONS FOR PART 2.5 (PART VI) WARRANTS		
		01/02	**02/03**	**03/04**

[27] Senate Legal and Constitutional Legislation Committee, above n 8, para 5.9.

AUSTRALIAN FEDERAL POLICE	Made Refused/withdrawn Issued	556 1 555	691 1 690	671 11 660
NATIONAL CRIME AUTHORITY	Made Refused/withdrawn Issued	274 0 274	164 0 164	- - -
AUSTRALIAN CRIME COMMISSION	Made Refused/withdrawn Issued	- - -	221 0 221	390 0 390
NEW SOUTH WALES CRIME COMMISSION	Made Refused/withdrawn Issued	644 0 644	803 5 798	827 3 824
INDEPENDENT COMMISSION AGAINST CORRUPTION	Made Refused/withdrawn Issued	55 0 55	38 0 38	31 0 31
NEW SOUTH WALES POLICE	Made Refused/withdrawn Issued	392 0 392	383 1 382	470 7 463
POLICE INTEGRITY COMMISSION	Made Refused/withdrawn Issued	36 0 36	81 0 81	62 0 62
SOUTH AUSTRALIA POLICE	Made Refused/withdrawn Issued	54 0 54	42 0 42	126 0 126
VICTORIA POLICE	Made Refused/withdrawn Issued	343 2 341	406 0 406	269 0 269
WESTERN AUSTRALIA POLICE	Made Refused/withdrawn Issued	148 1 147	190 2 188	182 4 178
WESTERN AUSTRALIAN ANTI-CORRUPTION COMMISSION	Made Refused/withdrawn Issued	16 0 16	48 0 48	22 4 18
WESTERN AUSTRALIAN CORRUPTION AND CRIME COMMISSION	Made Refused/withdrawn Issued	- - -	- - -	9 2 7

TOTAL	**Made** **Refused/withdrawn** **Issued**	**2518** **4** **2514**	**3067** **9** **3058**	**3059** **31** **3028**

2.4 Types of warrants

2.4.1 Service and named person warrants

Both Part 2.2 warrants and Part 2.5 warrants may be issued in respect of a telecommunications service or a person.[28] Service warrants are issued in relation to a particular 'telecommunication service' where there is a relevant connection between the person of interest and the service.[29] Where a person of interest is using more than one telecommunication service, there is provision for the issue of a named person warrant, which authorises the interception of those telecommunications services in relation to a particular person of interest.

2.4.2 Device warrants

The 2006 amendments have broadened the scope of named person warrants to authorise the interception of communications that are made by means of a 'telecommunications device' used by the person of interest. A 'telecommunications device' is defined as 'a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system' (s 5(1)). The Second Reading speech gives examples of mobile handsets and computer terminals. The issuing

[28] See ss 9, 9A, 11B, 11C, 45, 45A, 46, 46A. In relation to the collection of foreign intelligence there are foreign communications warrants which authorise broader interceptions than service or named person warrants (s 11C).

[29] 'Telecommunication service' is defined to mean 'a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication' (s 5).

authority must not issue a telecommunications device warrant unless 'there are no other practicable methods available' at the time of making the application to identify the telecommunications services used by the person of interest or the interception of a telecommunications service 'would not otherwise be practicable' (ss 9A(3); 46A(3)).[30] The Explanatory Memorandum said this amendment was designed 'to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.'[31]

The enactment of this measure was met with some controversy as to whether technology has developed to a point which would allow devices to be identified with sufficient precision, and the potential impact upon the privacy of innocent persons where the device identification cannot be determined with such precision.[32] The Blunn Report considered the difficulties of identifying a service being used by a person of interest, particularly the problems associated with the trading of SIM cards. The Report concluded that the 'SIM card and its associated service number is not an effective method of identification'.[33] The Report recommended that 'priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access'.[34] It was suggested that the International Mobile Equipment Identifier ('IMEI') presented a possible system of identification. The Report also indicated that the existing legal regime of named persons warrants may need to be changed to accommodate these developments.[35] Having heard the

[30] The Explanatory Memorandum said that this latter situation 'covers instances in which agencies may be able to identify all services, but is impractical to intercept each service. For example, a person of interest may transfer hundreds of different Subscriber Identity Module (SIM) cards through a mobile handset in quick succession. Interception of each telecommunications service (currently identified by reference to the SIM card) is extremely impractical to achieve before the person of interest changes the SIM card being used' (Explanatory Memorandum, Telecommuncations (Interception) Bill 2006 (Cth) 34.)

[31] Explanatory Memorandum, Telecommuncations (Interception) Bill 2006 (Cth) 34.

[32] See Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 12 March 2006 (Electronic Frontiers Australia), noted in Senate Legal and Constitutional Legislation Committee, above n 8, para 4.118.

[33] Blunn, above n 1, para 2.2.

[34] Ibid para 3.3.5.

[35] Ibid para 3.2.3-3.2.4.

evidence of officers from the Attorney-General's Department and the Australian Federal Police ('the AFP') as to the steps that will be required to be taken by warrant applicants to show a unique identifier, the Senate Committee was not entirely convinced that 'the device being targeted under the warrant was able to be certified as uniquely identifiable'.[36] Nevertheless, the Committee considered that the operational requirements for law enforcement officers warranted the introduction of the provisions at this time. The technological development needed to have a unique and indelible identifier of the source of telecommunications would take some time,[37] and operational needs, it would seem, justified any potential impact on the privacy of innocent parties.

2.4.3 B-Party warrants

Privacy interests have also been significantly affected by the new B-Party provisions inserted by the 2006 amendments. National security telecommunications service warrants under Part 2.2 and Part 2.5 telecommunications service warrants are now available not only in relation to 'persons of interest' but, following the 2006 amendments, also in relation to other innocent third parties who use a telecommunications service to communicate with the person of interest. For Part 2.2 warrants, interception of a telecommunications service may be authorised where the service 'is being or is likely to be the means by which a person receives or sends a communication from or to' a person of interest and the interception 'will, or is likely to, assist' ASIO in its security intelligence gathering functions (s 9(1)). In relation to Part 2.5 warrants, the issuing authority can issue a warrant in respect of a telecommunication service used by an innocent person where information 'that would be likely to be obtained' by the interception 'would be likely to assist' in connection with the investigation of a serious offence, in which another person is involved and with whom the innocent person 'is likely to communicate' (s 46(1)).

These circumstances that trigger the issue of a warrant are very broad, and once the warrant has been issued under either Part 2.2 or 2.5, there

[36] Senate Legal and Constitutional Legislation Committee, above n 8, para 4.122.

[37] Ibid para 4.125.

is little limitation on the type of communication that may be intercepted. There are no limitations as to the identity of the innocent party who uses the telecommunications service, the content of communication that may be intercepted, or the identity of other parties to the intercepted communication. For example, the B-Party might be the suspected person's legal representative with the result that the interception may lawfully capture otherwise privileged communications. It is also wide enough to capture the privileged communications between the legal representative and other clients, as well as collateral intimate communications between the legal representative and spouse, which have no bearing on the investigation. Alternatively, the B-Party may be the suspected person's medical practitioner or religious leader, and the intercepted communication may include communication by the medical practitioner with other patients or by the religious leader with other members of the religious community.

From a law enforcement perspective, it could be argued that anything short of full interception would impose significant burdens upon security and law enforcement agencies to filter out what might be considered to be unrelated communication. From a privacy perspective, the collateral damage to innocent third parties can be limited – indeed, the US federal wiretap regime generally (18 USC § 2510, Ch 119 (1994)) imposes a duty of minimisation on law enforcement officials: 'Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days'. In the Australian context, a policy of minimisation has never been given serious consideration, though there are statutory positions like the Public Interest Monitor (PIM) used in Queensland, that would be suitably qualified (both in terms of high security clearance and promotion of privacy interests) to perform this role. The role of the PIM is discussed below at 4.4.

There are some constraints placed upon the issuing authority. The issuing authority must not issue the warrant unless 'all other practical methods of identifying telecommunications services' used by the person

of interest have been exhausted or interception of communications used by the person of interest 'would not otherwise be possible' (ss 9(3), 46(3)). The Second Reading Speech said that:

> [t]his amendment will assist interception agencies to counter measures adopted by persons of interest to evade telecommunications interception, such as adopting multiple telecommunications services. The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by suspects.[38]

There is also the power to impose conditions or restrictions (ss 9(1); 49(1)). Although there is some evidence in the Attorney-General's reports to Parliament that conditions and restrictions have been imposed to protect privacy in relation to Part 2.5 warrants, the cases in which these have been imposed are very few.[39]

In recognition of the potential privacy intrusion for non-suspects, the time periods for B-Party warrants under both Part 2.2 and Part 2.5 are half the periods of other service warrants.[40]

The provisions are extremely broad in their scope and, unsurprisingly, attracted considerable attention during the Senate Committee review of the amendment. The potential intrusion on the privacy of innocent third persons was criticised in a number of submissions to the Committee. Indeed, the Australian Privacy Foundation complained that the B-Party amendment had come 'out of the blue'.[41] While the Blunn Report had discussed B-Part interceptions, it was in the context of uncertainty as to

[38] Commonwealth of Australia, *Parliamentary Debates*, House of Representatives, 16 February 2006 (P Ruddock) 8.

[39] See *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004,* paras 4.13-4, Table 5.

[40] Whereas ASIO may seek a telecommunications service under Part 2.2 for a period of six months, B-Party warrants are only available for three months. Similarly, while law enforcement officers can seek a Part 2.5 warrant for 90 days, B-Part warrants under Part 2.5 may only be issued for 45 days (see ss 9B(3A) and 49(3)).

[41] Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006, (Australian Privacy Foundation) 8.

whether B-Party interceptions were allowable under the provisions in their form at that time. Blunn recognised that law enforcement agencies interpreted the provisions as not allowing B-Part intercepts, but referred to Federal Court authority upholding the validity of B-Party warrants.[42] The potential impact on privacy associated with the use of B-Party warrants should not, it was said, 'depend on non-judicial interpretation of the relevant sections, the meaning of which is certainly open to argument'.[43] It was in that context that the Blunn Report recommended that the Act 'be amended to clarify that B-Party services may be intercepted in *limited and controlled circumstances*'.[44] Blunn, however, made it clear that there are 'obvious and serious privacy implications involved' and that controls must be put in place to prevent the use of B-Party intercepts as 'fishing expeditions'.[45]

The Senate Committee expressed concern about the potential privacy invasion:

> … the Committee accepts the need for B-party warrants. However, the invasion of privacy of innocent parties who become the subject of surveillance merely by reason of association is very significant. The key question is therefore the extent to which the Bill provides a framework for controls over the proposed warrants to balance privacy protection with effective law enforcement.[46]

The Committee recommended various amendments to confine the scope of B-warrants. These recommendations included:

- a requirement for a stronger nexus between the information intercepted and security intelligence gathering and law

[42] Blunn, above n 1, paras 12.1-12.10. Blunn referred to the Federal Court case of *Flanagan v Commissioner of the Australian Federal Police* (1995) 60 FCR 149.

[43] Ibid para 12.7.

[44] Ibid para 12.10 (emphasis added).

[45] Ibid paras 12.6-12.9.

[46] Senate Legal and Constitutional Legislation Committee, above n 8, para 4.27.

enforcement purposes before a warrant can be issued;[47]

- that agencies exhaust all other methods of identifying the communications services used, rather than exhausting all other 'practicable' methods;[48]

- that B-Party warrants cannot be renewed;[49]

- that certain communications be exempted from B-Part warrants (including communications between lawyer and client; clergy and devotee; doctor and patient and communications by the B-Party with any person other than the person of interest);[50]

- that there be limits on the subsequent use of intercepted communications;[51]

- that there should be stricter supervision of destruction of non-material content;[52]

- that B-Party statistics be separately recorded by each agency and separately reported to Parliament;[53]

- that the B-Party provisions expire after five years and that they be reviewed prior to or at that time;[54] and

- that such a review look more broadly at the use of AAT members to

[47] Ibid Rec 18, para 4.43; Rec 19, para 4.56.

[48] Ibid Rec 20, para 4.57.

[49] Ibid Rec 21, para 4.61.

[50] Ibid Rec 22, para 4.80.

[51] Ibid Rec 23, para 4.81.

[52] Ibid Rec 24, para 4.97.

[53] Ibid Rec 24, para 4.97.

[54] Ibid Rec 25, para 4.111.

issue warrants and issues of emerging technologies.[55]

Of these recommendations, only the enhanced recording and reporting requirements were adopted by the government in its Senate amendments. Attempts by the Opposition and Democrats to implement the other recommendations were not supported by the government.

2.5 Part 2.5 warrants and privacy considerations

When considering applications for Part 2.5 warrants, the issuing authorities are required to take a range of considerations into account.[56] Prior to the 2006 amendments, the considerations were broadly similar in relation to Class 1 and Class 2 offences, except that the potential invasion of privacy was not a consideration required to be taken into account for warrant applications in relation to Class 1 offences. We have previously observed this to be anomalous, as the need for specific consideration of privacy interests does not diminish with the increased seriousness of the offence under consideration – indeed, there are plausible arguments that the privacy interest become of greater rather than of lesser significance.[57] The Blunn Report recognised that privacy considerations should be a matter to be considered in all Part 2.5 warrant applications.[58] The Second Reading Speech accompanying the amendments[59] and the Senate Committee Report[60] also recognised the positive outcome for privacy protection following the removal of the distinction between Class 1 and Class 2, and the requirement to consider privacy considerations in all cases. In light of the low rate of refusal for warrants across both classes, the reality, as the Blunn Report recognised, is that 'privacy considerations

[55] Ibid Rec 25, para 4.112.

[56] Privacy considerations are not matters expressly to be considered by the issuing authority in relation to Part 2.2 warrants.

[57] S Bronitt and J Stellios, "Telecommunications Interception in Australia: Recent Trends & Regulatory Prospects" (2005) 29 *Telecommunications Policy* 875, 885.

[58] Blunn, above n 1, para 6.4.

[59] Commonwealth of Australia, *Parliamentary Debates,* House of Representatives, 16 February 2006.

[60] Senate Legal and Constitutional Legislation Committee, above n 8, para 5.9.

are unlikely to preclude the issue of a warrant for any of the offences characterised as Class 1 offences or indeed for many of the Class 2 Offences'.[61]

2.6 Interception – prohibition on subsequent use of intercepted communications

The second prohibition in the interception regime is at the stage of subsequent use of intercepted material. Section 63(1) prohibits the communication, use or recording of intercepted information. The primary exceptions from the prohibition include the communication of lawfully intercepted information for security (ss 64, 68(a)) and law enforcement purposes (s 68), and the communication by ASIO of foreign intelligence information (s 64). Law enforcement purposes include the investigation or prosecution of a serious offence or any offence punishable by imprisonment for life or for a period of at least 3 years (ss 5 and 67). Lawfully intercepted information may also be given in a range of proceedings, including a prosecution of any serious offence or offence punishable by imprisonment for life or for a period of at least 3 years (ss 5B and 74). Thus, while the lawful interception of communications may only be in relation to serious offences, lawfully intercepted information may be used for the investigations of, and given in proceedings for, lesser offences. Importantly, the offence which is the subject of the investigation or prosecution need not be connected to the serious offence which motivated the lawful interception. Once that information is given as evidence in an exempt proceeding, it may then be given in any proceeding (s 75A).

2.7 Destruction, record keeping and reporting requirements

Section 79 of the Act imposes destruction obligations on the AFP and the Australian Crimes Commission ('ACC'). Where the chief officer of the agency is satisfied that a restricted record[62] 'is not likely to be required for

[61] Blunn, above n 1, para 6.4.

[62] Defined as 'a record other than a copy, that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system'.

a permitted purpose', the records must be destroyed 'forthwith'. The AFP and ACC are also required to keep detailed records of the warrants that have been issued and the use made of intercepted information (ss 80 and 81). The same requirements are imposed on State authorities as preconditions to being authorised to apply for Part 2.5 warrants (s 35(1)(a), (f), (g)).

In relation to Part 2.5 warrants, the Commonwealth Ombudsman is given the responsibility of inspecting the records of Commonwealth agencies in order to ascertain compliance with destruction and record-keeping obligations (s 83). The Ombudsman must report to the Attorney-General within three months of the end of each financial year (s 84), and may report on any other breach of the Act (s 85). In relation to State agencies, regular inspections must be undertaken by an independent State authority, with reports being given to the Commonwealth Attorney-General (s 35(1)(h)-(m)). As indicated above, these are preconditions to being authorised to apply for Part 2.5 warrants. Commonwealth and State agencies also must give annual reports to the Commonwealth Attorney-General in relation to Part 2.5 interception warrants and the use made of intercepted information (ss 94 and 96). The Attorney-General must then report on these matters to Parliament.[63]

Prior to the 2006 amendment, the Commissioner of the AFP had the responsibility of keeping registers of Warrants, containing information about Part 2.5 warrants. That responsibility is now to be exercised by the Secretary of the Attorney-General's Department. The effect of the amendments is that all Part 2.5 warrants (whether issued by Commonwealth or State agencies) must be notified to the Secretary of the Attorney-General's Department (s 53(1)).[64]

In relation to Part 2.2 warrants, the Inspector-General of Intelligence and Security conducts inspections of all requests for warrants under the *Inspector-General of Intelligence and Security Act 1986* (Cth).

[63] At the time of writing, the most recent report is for the period ending 30 June 2004.

[64] With the repeal of s 54, all Part 2.5 warrants now come into force upon issue.

3 (Data)veillance laws: the new stored communication scheme

3.1 Introduction

The 2006 amendments introduced provisions for the protection of stored communication, though permitting access to the material under defined conditions. The scheme broadly contains similar prohibitions, exceptions and reporting requirements to those contained in the interception provisions, although with important differences. The introduction of these provisions followed a protracted attempt by the government to amend the TI Act to deal with stored communications. In 2002 and again in 2004, the government sought amendments to remove the requirement for a warrant where stored communications could be accessed without the use of a telecommunications line. There followed disagreement between the Commonwealth Attorney-General's Department and the AFP on how the existing interception provisions were to be interpreted. The central issue was whether a stored communication had ceased 'passing over the telecommunications system'. The Department's position was that the accessing of communications prior to reaching the recipient's receiving terminal (e.g., from internet service providers) constituted a contravention of the interception provisions, whereas the AFP was of the view that such information could be accessed using the warrants provision in s 3L if the *Crimes Act* (Cth). On this latter view, governmental agencies could use their general statutory access and notice to produce powers in relation to accessing such information.

In the face of continuing disagreement over the proposed amendment, the Senate Legal and Constitutional Legislation Committee recommended an independent review of the position, and that the status quo be maintained until that review was undertaken.[65] The *Telecommunications (Interception) Amendment (Stored Communications)*

[65] See Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment Bill 2004* (2004); Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (2004).

Act 2004 (Cth) was enacted to exclude stored communications from the interception prohibition (s 7(2)(ad)). In recognition that this was to be an interim measure, the 2004 amendment was subject to a 12 month sunset clause and, thus, was to cease operation on 14 December 2005. To allow the government sufficient time to implement the Blunn recommendations, the sunset date was extended to 14 June 2006 by the *Telecommunications (Interception) Amendment (Stored Communications and other measures) Act 2005* (Cth).

Blunn accepted that there was a distinction between intercepting real-time communications and accessing stored communications, although he acknowledged that there may seem to be little difference from a privacy point of view. Real-time voice communications, it was said, 'are likely to be more spontaneous than other forms of data communication and do not provide the opportunity for "second thoughts" prior to transmission offered by those other forms'.[66] The Report recommended that the distinction be maintained.[67] Although it was recognised that much of modern communication passing over the telecommunications system is not voice communication, Blunn considered it 'impractical and undesirable' to suggest different regimes for real-time access (i.e., interception) depending on whether the communication is voice or in some other form.'[68]

The Blunn Report also recognised that access to stored communications was inadequately regulated by other legislation. While law enforcement agencies could access such information for their purposes, there was insufficient privacy protection in the access authorisation, and the storage and disposal processes.[69] Blunn recommended that a warrant scheme should be enacted with similar elements to those existing for interceptions, including access by warrants

[66] Blunn, above n 1, para 1.4.2.

[67] Ibid para 1.4.3.

[68] Ibid para 1.4.4. A similar approach was recommended by an earlier review of the US federal wiretap laws: *The Electronic Frontier: The Challenge Of Unlawful Conduct Involving The Use Of The Internet - A Report Of The President's Working Group On Unlawful Conduct On The Internet* (March 2000): http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#ECPA.

[69] Ibid para 1.8.1.

issued by independent issuing authorities who are to consider privacy implications; regulation of subsequent use; and storage and destruction provisions.[70] Importantly, Blunn was of the view that the data access procedures should apply not only to communications stored within the system, but also information stored in electronic equipment in the possession of the intended recipient. For Blunn, the privacy issues applied equally to both.[71]

3.2 The prohibition on accessing stored communication

Purporting to implement these Blunn recommendations, s 108 of the TIA Act prohibits the accessing[72] of stored communication without the knowledge of either the intended recipient or the sender of the communication.[73] It is sufficient to have knowledge for these purposes if a written notice has been given to the person (s 108(1A)). The knowledge element preserves other overt access mechanisms which involve the knowledge of one of the parties to the communication.[74]

The definition of 'stored communication' has been amended to mean a communication that is not passing over a telecommunications system, is held on equipment operated by a carrier, and cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier (s5(1)). The amended definition is intended to clarify that the provisions do not cover access to information that involves the knowledge of a party (i.e., overt access) or which does not require the assistance of an employee (i.e., access to

[70] Ibid para 1.6.1.

[71] Ibid para 1.6.3.

[72] 'Accessing' a stored communication consists of 'listening to, reading or recording such a communication, be means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication' (s 6AA).

[73] The amending provision originally referred only to the knowledge of the recipient, but was amended in the Senate: Commonwealth of Australia, *Parliamentary Debates,* Senate, 29 March 2006, 86; Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 3.

[74] See discussion ibid 2.

voicemail or text message where a mobile phone is seized from a suspect's premises).[75]

3.3 The warrant provisions

There is a range of exceptions to the prohibition on accessing stored communications, primarily those allowing access under an interception warrant (s 108(2)(b)) or a stored communications warrant (s 108(2)(a)). The former essentially operates to expand the authority of an interception warrant to cover stored communication that would have been covered by the interception warrant if it were still passing over a telecommunications system (s 108(3)). As the Explanatory Memorandum said, '[i]n the absence of this exception, interception warrants, which only operate prospectively from the time they are served on the carrier, would not authorise access to stored communication previously sent, meaning that an agency would need to also obtain a stored communication warrant to ensure complete access to all communications'.[76] Access to stored communications for ASIO is authorised in this way: the authority of Part 2.2 interception warrants is extended to cover stored communications (s 109).

However, because there is a broader group of enforcement agencies who can apply for a stored communications warrant than those entitled under Part 2.5, Part 3.3 sets out a separate stored communication warrant system for enforcement agencies. Issuing authorities can issue stored communications warrants in respect of a person where there are reasonable grounds for suspecting that a carrier holds stored communications to or from the person, and information 'that would be likely to be obtained' from access 'would be likely to assist in connection with the investigation' of 'a serious contravention in which the person is involved' (s 116). In deciding whether to issue the warrant, the issuing authority is to consider a range of matters including privacy

[75] Supplementary Explanatory Memorandum, Telecommunications (Interception) Bill 2006 (Cth) 2. As the note to s 108 says, the section 'does not prohibit accessing of communications, that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient'.

[76] Explanatory Memorandum, *Telecommunications (Interception) Bill 2006* (Cth) 10.

considerations. There is the possibility for conditions and restrictions to be placed upon the warrant (s 117).

Although resembling the broad framework of interception warrants, there are important differences. First, issuing authorities include not only federal court judges and AAT members, but also State magistrates (s 6DB). Secondly, additional agencies may apply for stored communication warrants. In addition to those entitled under the interception provisions, all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue may apply for a stored communications warrant.[77] The Explanatory Memorandum suggests that these agencies would include the Australian Customs Services, the Australian Tax Office, the Australian Securities and Investment Commission, and similar State and Territory agencies.[78] Unlike the framework under the interception regime, there is no Commonwealth vetting mechanism for State agencies. As discussed above, on satisfaction that State agencies have requisite inspection and reporting mechanisms in place, the Attorney-General can declare a State agency to be eligible to apply for interception warrants. No such mechanism applies under the stored communication provisions.

Thirdly, warrants may be sought in relation to 'serious contraventions'. These are defined to include not only 'serious offences' as in the case of interception warrants, but also offences punishable by imprisonment for at least three years or a fine of at least 180 penalty units (or 900 in the case of a corporation); and statutory contraventions that give rise to a pecuniary penalty or equivalent monetary liability of 180 penalty units (or 900 in the case of a corporation) (s 5E). Fourthly, as will be considered further below, reporting requirements for stored communication warrants are not as burdensome.

The broadening of the access regime and the relaxation of various thresholds in relation to stored communications appeared to be justified

[77] 'Enforcement agencies' are defined (see s 5(1)) by reference to s 282 of the *Telecommunications Act 1997* (Cth). Potentially, many agencies of State and Territory government could be granted access to these warrants for the purpose of enforcing any law which carry the prescribed pecuniary penalties.

[78] Explanatory Memorandum, *Telecommunications (Interception) Bill 2006* (Cth) 12.

primarily on the basis of a perceived difference between real-time and stored communications, a distinction made in the Blunn Report. Blunn focused on the distinction between 'spontaneous' forms of communication and forms of communication which allowed for 'second thoughts'. This was reflected by the responses by the Attorney-General's Department to the Senate Committee when quizzed about the Blunn distinction between real-time and stored communication:

> Mr McDonald [Assistant Secretary, Attorney-General's Department]: I had some quite interesting discussions with Mr Blunn about this issue, and it is not an easy one, but certainly the idea that it is slightly more considered is something that was in his mind or was something that we discussed. It is something that is in writing – something that definitely involves more consideration of the expression – although there is the speed issue.[79]

Mr McDonald then explained that some written forms like text messaging can be sent quite quickly.

However, there is a number of difficulties with the making of that distinction. Even if one accepts the rationale, that written forms of communication involve more consideration or reflection, the live/stored distinction is not a good approximation for the spontaneous/considered distinction that Blunn had in mind. Both live communication and stored communication may comprise forms of spontaneous and considered communication. In fact, the amendments recognise this by extending the authority of interception warrants to cover stored communications. However, as alluded to by Mr McDonald of the Attorney-General's Department, the assumption that the written form is more considered does not hold as a general rule. This point was the subject of discussion during the Senate Committee process and the Senate debate.[80] The opposition to such a distinction was well illustrated by Senator Stott Despoja's comments during the course of the Senate debates: '[t]he premise that more consideration or thought may be put into an SMS, an

[79] Evidence to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 15 March 2006, (Geoffrey McDonald) 55.

[80] See, for example, Evidence to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 15 March 2006, (Prof George Williams) 28, 31.

email message or a message left on voicemail in comparison to a telephone conversation is, in this day and age, spurious.'[81]

In any event, even if one were to accept the spontaneous/considered distinction, and that the live/stored distinction was a reasonable approximation, it might still be argued – as Blunn accepted – that from a privacy perspective, there is no relevant difference that would justify different levels of protection.[82] Clearly, as the Blunn Report concluded, the mode of expression does not alter the reasonable expectation of privacy in respect of such personal communications. Moreover, it is possible to argue that law enforcement access to stored communications (email, SMS messages, etc) enlivens an even stronger privacy interest: in these cases, the state is seeking access to past communications that record thoughts and behaviours of individuals over a much longer period (if measured in the equivalent of real-time) than the standard three months of prospective surveillance permitted under interception warrants. In such cases, the conditions of access to such material should be more rather than less stringently enforced.

The Senate Committee accepted that the relevant distinction in this context is between covert and overt searches, and the guiding test should be the impact on individual privacy.[83] Given the significant impact of covert access on privacy, and considering that the wider group of enforcement agencies have access to covert access methods,[84] the Committee recommended that: (i) enforcement agencies able to access stored communications should be limited to those eligible under the interception provisions;[85] (ii) States enact complementary legislation as a

[81] Commonwealth of Australia, *Parliamentary Debates,* Senate, 28 March 2006.

[82] See Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, March 2006 (New South Wales Council for Civil Liberties) 3; Australian Privacy Foundation above n 26, 5.

[83] Senate Legal and Constitutional Legislation Committee, above n 8, para 3.39.

[84] In fact, ASIC had provided information that '[t]he majority of … access to emails [came] from access at the user's end' and that in the previous 12 months it had not accessed stored communications from an internet service provider: ibid paras 3.36-7.

[85] Ibid Rec 2, para 3.42.

precondition to being entitled to apply for a warrant;[86] (iii) warrants be limited to criminal offences;[87] and (iv) issuing authorities be limited to those under the interception provisions.[88]

The government did not seek to implement these recommendations, and did not support the Opposition and Democrat amendments seeking to do so. In rejecting these amendments and a correspondence of live and stored communication, Senator Ellison said that:

> to compare stored communications with a communication that is taking place is somewhat unreal. … [O]nce a message or communication has been transmitted it is of a different nature to one that is in process. That is precisely what was acknowledged by Mr Blunn in his report when he acknowledged the difference between real-time interception and a communication that has been received.[89]

However, given the discussion above, if a transmitted communication is *different in nature* to a communication whilst in transmission, that rationale is yet to be provided.[90]

3.4 Prohibition on subsequent use

The prohibition on subsequent use of stored communication information and related exceptions broadly mirror those for the interception scheme. Stored communication information cannot be communicated, used, recorded or given in evidence in a proceeding (s 133). The principal exceptions include the communication of lawfully

[86] Ibid Rec 6, 3.67. Or, at least as an interim measure, that the definition of enforcement agency be amended to allow an agency to be excluded from being able to obtain a stored communication warrant (Rec 7, para 3.68).

[87] Ibid Rec 3, 3.43.

[88] Ibid Rec 5, 360.

[89] Commonwealth of Australia, *Parliamentary Debates,* Senate, 29 March 2006 (Sen. Chris Ellison) 42.

[90] It should be noted that Senator Ellison also tried to justify the different treatment on the basis that an interception warrant involves ongoing monitoring, whereas a stored communication warrant involves access at a fixed point in time to information already received (ibid). While there may be such a difference, it still remains unclear why this should be a relevant consideration supporting less stringent treatment for stored communications warrants. To the contrary, the retroactive nature of stored communications warrants may suggest that more stringent measures be put in place for stored communications warrants.

accessed information for security (ss 136, 137) and law enforcement purposes (s 68), and the communication by ASIO of foreign intelligence information (ss 136, 137). Law enforcement is, however, much broader than under the interception provisions. The permitted purposes include investigations and prosecutions for offences punishable: by imprisonment for a period of 12 months or by a fine of at least 60 penalty units (or 300 penalty units in the case of corporations); and investigations and proceedings for recovery of pecuniary penalties of at least 60 penalty units (or 300 penalty units in the case of corporations) (ss 5B and 143). Lawfully accessed information may also be given in a range of proceedings. Again, the proceedings are broader than those under the interception provisions (ss 5B and 143). As with the interception provisions, the threshold for subsequent use is lower than the warrant thresholds, and subsequent use need not be connected to the purpose for which the information was accessed. Once that information is given in evidence in an exempt proceeding, it may then be given in any proceeding (s 145).

3.5 Destruction, record keeping and reporting requirements

Similar to the interception provisions, stored communication information in the possession of an enforcement agency, must be destroyed 'forthwith' where the information is no longer required for the relevant purpose (s 15). However, there are important differences in relation to the record keeping and reporting requirements for stored communications warrants when compared with those discussed above in relation to interception warrants. First, while enforcement agencies have to keep records, the content of those records are not required to be as detailed as those under the interception provisions. Secondly, the information to be provided by enforcement agencies to the Attorney-General, and then reported by the Attorney-General to Parliament, is also significantly less detailed (ss 162 and 163). Thirdly, as noted earlier, there is no equivalent mechanism to that in the interception provisions that requires a State agency to have record keeping and reporting mechanisms in place as preconditions to accessing the stored communications warrants. The less burdensome requirements were said

in the Explanatory Memorandum to reflect 'the wider agency access and the lower threshold to be met'.[91]

These less burdensome requirements were the subject of criticism through the Senate Committee process and in the Committee's report. In response, the Committee emphasised that the 'reporting obligations are vital to provide adequate transparency and accountability for the stored communications warrant regime' and that 'a lower offence threshold does not equate to a lesser reporting obligation'.[92] The Committee recommended that the 'Bill be amended to require agencies and the [Attorney-General] to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants'.[93] The Committee also recommended that time limits be included within the legislation for the review and destruction of stored communication information.[94]

The government, however, did not implement these recommendations, and the Opposition and Democrat proposed amendments designed to give them effect, were not supported by the government in the Senate. In opposing the amendments, Senator Ellison said:

> We believe that the reporting proposed by the government is sufficient. When you look at the [TI Act] reports that are being furnished to the parliament, they are indeed detailed … It is a comprehensive report. We believe that to go as far as the Democrats are suggesting could well have some operational impact and we are not inclined to support these amendments.[95]

It appears that the 'operational impact' the Senator had in mind was that organised criminals would be able to track the trends of law

[91] Explanatory Memorandum, Telecommuncations (Interception) Bill 2006 (Cth) 13.

[92] Senate Legal and Constitutional Legislation Committee, above n 8, para 3.88.

[93] Ibid Rec 11, para 3.91.

[94] Ibid Rec 10, para 3.81.

[95] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006 (Sen. Chris Ellison) 28.

enforcement revealed in the annual reports, and change their methods accordingly.[96] When pressed further by Senator Stott Despoja on how the 'basic' statistical information revealed in the interception reports might create operational problems,[97] Senator Ellison replied that the Senate Committee's recommendation about reporting requirements are still being considered, and that Senator Stott Despoja's concerns would be 'taken on board'.[98] If the 'operational impact' is affecting policy development in this way, there is a real danger that future amendments might, in fact, go the other way and lower the reporting requirements for interceptions as well.

Finally, the Ombudsman is given an inspection and reporting role in relation to stored communications warrants issued to enforcement agencies (s 153). The Ombudsman must report on agency compliance with record-keeping and enforcement obligations within three months after the end of each financial year. During the Senate Committee inquiry, the Ombudsman submitted to the Committee his concern that the expanded role would impose an additional burden on the resources of his office. Professor McMillan indicated that it would be likely that greater resources would be necessary to complete the additional functions, and that it would be useful if the reporting deadline under the stored communication regime be extended from three to six months.[99] The Senate Committee supported these requests.[100] In declining to support Opposition and Democrat amendments to give effect to these recommendations, Senator Ellison said: '[the government] sees no reason to delay the report of the Ombudsman – in fact, it should be reporting which is fairly expeditious'. Although recognising that the government would continue to consider the Committee's recommendations, the Senator concluded that '[a]t this stage, there is no

[96] Ibid 28-9.

[97] Ibid 29.

[98] Ibid 30.

[99] Submission to Senate Legal and Legislation Committee, Parliament of Australia, Canberra, March 2006 (Commonwealth Ombudsman) 2-3.

[100] Senate Legal and Constitutional Legislation Committee, above n 8, Rec 12 and 13, paras 3.92 and 3.93.

compelling reason … to agree to this amendment'.[101]

4 Balancing away privacy interests

4.1 Introduction

We have previously observed that various developments since the enactment of the TI Act have placed considerable pressure on privacy in a way not initially contemplated. The regulatory landscape has shifted to such an extent that there is no longer a position that resembles a 'balance'. We called for legislative reform that places rights protection - which extend beyond privacy to include rights for a fair trial and due process - at the centre of regulatory design.[102]

The response to such calls seemed promising, at least in respect of privacy. In his findings, Blunn said that 'the protection of privacy should continue to be a fundamental consideration in, and *the starting point for*, any legislation providing access to telecommunications for security and law enforcement'.[103] The Senate Committee commenced its task with the following statement: '[t]he principal consideration of legislation which governs access to personal communications should be the protection of privacy'.[104]

Despite these statements, the government's approach remains one of 'balancing' privacy considerations with security and law enforcement objectives and, indeed, most of the parliamentary debate is couched in terms of finding the right 'balance'.

[101] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006 (Sen. Chris Ellison) 26. Ironically, this position was put forward shortly prior to the Senator's forced acknowledgment that the Attorney-General's report to Parliament for the year ending 30 June 2005 had not yet been reported to Parliament (ibid 28).

[102] Bronitt and Stellios, above n 42, 887.

[103] Blunn, above n 1, 5 (emphasis added).

[104] Ibid 7.

However, there is a growing recognition that a balancing approach to the legal regulation of covert surveillance is problematic. The New South Wales Law Reform Commission had initially taken the balancing approach, arguing that privacy interests must be weighed against legitimate societal interests in preventing and prosecuting crime.[105] It subsequently revised that approach following further research, concluding that the balancing approach was 'inherently flawed'.[106] Although a persistent idea in all areas of policy development, balancing models rarely achieve an accommodation between competing interests. In other law enforcement contexts, critical scholars have argued that 'balancing' tends to prioritise the interests of crime control over due process.[107] In the context of telecommunications interception, the balancing process has systematically traded-off privacy interests in favour of law enforcement.

The remainder of this paper will consider the extent to which privacy interests have been balanced away through the adoption of 'balancing' rhetoric. First, it will be seen that the accelerated passage of the 2006 amendments through Parliament did not allow for a proper consideration of the privacy implications (Part 4.2.). The Senate Committee process, which is often praised for the contribution that it makes during the legislative process towards rights-protection, was marginalised (Part 4.3.). Secondly, it will be seen that the two main mechanisms within the legislative scheme to protect the privacy interests of a person who is the subject of a warrant – the warrant system (Part 4.4.) and civil remedies (Part 4.5.) – are largely illusory. Thirdly, the 2006 amendments illustrate that, when the opportunity arises for a consideration of which interests should prevail, security and law enforcement objectives systematically prevail over privacy interests (Part 4.6.).

[105] New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No. 98 (2001).

[106] Ibid para 2.4.

[107] A Ashworth, ,Crime, community and creeping consequentialism [1996] 43 *Criminal Law Review*, 220-30; S Bronitt and D Roche, "Between Rhetoric and Reality: Sociolegal and Republican Perspectives on Entrapment" (2000) 4 *International Journal of Evidence and Proof* 77.

4.2 The process of 'balancing'

If the model of 'balancing' interests is to have any legitimacy, the process of law-making needs to be capable of taking various interests into account. The 2006 amendments to the TI Act, however, are an example of a process that did not adequately allow for a proper exploration of how the proposed law impacts upon competing interests.

The amendments were introduced into the House of Representatives on 16 February 2006, and were debated on the evening of 28 February and the morning of 1 March. The Bill was then introduced into the Senate on 1 March 2006 and was immediately referred to the Senate Legal and Constitutional Legislation Committee for review by 27 March. Written submissions were invited by 13 March, and a public hearing was held on 15 March. Only seven days notice was given for those wanting to provide written submissions, and only three days notice was given for those wanting to appear at the hearing. The Senate Committee reported on 27 March. The Senate debated various amendments on 27, 29 and 30 March, with the legislation passing the Senate with amendments on 30 March.

Various submissions to the Senate Committee complained about the lack of time to properly consider the amendments. The Law Society of South Australia said that '[t]he very short timeframe given for consideration of this major piece of proposed legislation is of great concern and has not allowed proper consultation and consideration of it'.[108] The Law Council of Australia said that '[i]n the context of the Bill, it is particularly important to provide reasonable time for consultation to ensure that the government can properly consider concerns of the Australian people and to achieve an appropriate balance between safeguarding fundamental human rights and the "threat to the Australian people"'.[109] Even the most comprehensive submission made by Electronic Frontiers Australia complained of insufficient time to consider

[108] Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 14 March 2006 (Law Society of South Australia) 1.

[109] Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 13 March 2006 (Law Council of Australia) 4.

all the amendments properly.[110] The Supplementary Report of the Australian Democrats to the Senate Committee's Report noted 'with dismay the lack of time that the committee had been allocated to report on the bill'.[111] The lack of time for both the Senate Committee and those submitting to the Committee was a frequent complaint by the Opposition, Democrats and Greens throughout the Senate debate.[112]

The government defended these attacks on the basis that urgent legislation was needed on stored communications before the sunset date of 14 June. While this may address the stored communication provisions, it provides an insufficient basis to explain why the other privacy-impacting amendments were pressed at that time in the face of opposition in Parliament and from the Senate Committee's bipartisan report. The government emphasised on a number of occasions through the parliamentary debates that this was the first step in the process of responding to the Blunn report, and that other recommendations from the Blunn report and the Senate Committee's report are the subject of ongoing review. It remains to be seen whether other privacy-protecting recommendations will be the subject of future amendments.

The speed with which the amendments were considered not only denied sufficient time for consideration of their impact, but it also at times created confusion within the Senate whilst amendments were being debated. The most obvious example was when the Senate was considering an Opposition amendment dealing with copies of stored communication. As explained above, the amendments introduced a new definition of stored communication. Electronic Frontiers Australia had argued to the Senate Committee that it was not clear whether a copy of a stored communication is to be regarded as a stored communication for the purposes of the Act. The Senate Committee recommended that the

[110] Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 12 March 2006 (Electronic Frontiers Australia), above n 17, 8.

[111] 'Supplementary Report with Additional Comments of Dissent by the Australian Democrats', Senate Legal and Constitutional Legislation Committee, Parliament of Australia, *Provisions of the Telecommunications (Interception) Bill 2006* (2006) para 1.4.

[112] See for example: Commonwealth of Australia, *Parliamentary Debates,* Senate, 28 March 2006, 54, 55, 76, 79; Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 29, 40.

Bill be amended 'to ensure that copies of communications can not be accessed without a stored communications warrant'.[113] The Opposition's amendment to implement this recommendation was supported by the Democrats, but opposed by the government. However, in explaining why the government opposed the amendment, it became clear that Senator Ellison misunderstood the nature of the amendment:

> I think Mr Tom Sherman covered this aspect in a report several years ago. The government considered it then and decided not to proceed with it. As I understand it, the agencies concerned have indicated that there is an administrative burden in this which far outweighs any benefit that might be provided by possible enhanced accountability.[114]

Senator Ellison was discussing a different point about extending the record keeping and destruction obligations under the TI Act to include copies of records. In his review of named person warrants in 2003, Tom Sherman had recommended that the definition of restricted record be amended to include copies of records.[115] There is no indication in the Senate debate that any of the parties recognised this misunderstanding.

Thus, in addition to the concerns expressed about time limitations affecting a proper consideration of the impact of the amendments, the speed with which the amendments were passed also impacted upon the capacity of legislators to understand the scheme being enacted. Both of these consequences have a negative effect on policy and legislative design. If the 'balancing' model is to be adopted, the process of law-making must provide a genuine opportunity for the balancing of competing interests.

4.3 The effectiveness of the Senate Committee system

Despite the limitations confronting the Senate Committee, its members displayed impressive comprehension of the legislative scheme and the

[113] Senate Legal and Constitutional Legislation Committee, above n 8, Rec 14, para 3.107.

[114] Commonwealth of Australia, *Parliamentary Debates,* Senate, 29 March 2006 (Sen. Chris Ellison) 130.

[115] Tom Sherman, *Report of Review of Named Person Warrants and Other Matters,* (Commonwealth of Australia, 2003) Ch 9. The definition had been amended by the *Telecommunications (Interception) Legislation Amendment Act 2000* (Cth) to exclude copies from the definition.

issues arising from the proposed amendments. The Committee produced a bipartisan report which responded to the key issues raised by the written and oral submissions. The Committee considered that, in a number of important respects, the proposed amendments tilted the balance too far away from the protection of privacy interests and recommended various amendments – many of which have been or will be discussed in this paper. The Democrat Supplementary Report dissented only in the sense that it sought further privacy protection within the legislative scheme.

While purporting to respond to the Committee's report, it is quite clear that the government's amendments in the Senate only reflected the privacy concerns of the Committee in a limited way. The only privacy enhancing recommendation incorporated by the government into its amendments was for B-Party warrant statistics to be separately reported to Parliament.[116] The Opposition and the Democrats sought to introduce further amendments in an attempt to implement other Committee recommendations, however, none of these attempts were supported by the government, including Senators who supported the amendments as members of the Senate Committee. This turnaround led Senator Stott Despoja to say during the Senate debates:

> We have backbenchers in here today who signed off on the legislative report but were forced [to] vote against the recommendations contained in that report. Doesn't anyone have a problem with that? I think that is quite extraordinary. Some of the safeguards built into that majority report and proposed for legislation have since been voted against by the people who mooted them. Maybe the Senate committee process is a farce now.[117]

The government defended its lack of support for further amendments to implement Committee recommendations on the basis that the recommendations are the subject of ongoing review. Thus, the telecommunications interception context may provide an early test to see

[116] See Senate Legal and Constitutional Legislation Committee, above n 8, Rec 24, para 4.97. There was some debate in the Senate as to how many Senate Committee recommendations the government had adopted: see Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 1-2.

[117] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 200, 43.

whether the Senate Committee process will serve a useful role in an era of government control of the Senate.

4.4 Safeguarding privacy through warrants

The warrant system in Australia is often presented as an important safeguard for the protection of privacy interests. Following the 2006 amendment, privacy protection is a factor to be taken into account in the issuing of all Part 2.5 interception warrants and stored communications warrants. Although it is not a factor expressly to be taken into account by an issuing authority in relation to Part 2.2 warrants, the legislative scheme does not preclude consideration of the impact upon privacy. There are, however, some problems with seeing the warrant system as providing an effective bulwark against arbitrary intrusion into privacy.

First, as noted above, the Blunn report said that privacy considerations are unlikely to outweigh security and law enforcement considerations. This observation is supported by the experience with Part 2.5 warrants. Table 1 shows the application statistics for the last three reporting years. The figures clearly show that an almost negligible percentage of applications are refused or withdrawn. The figures are not further broken down into percentage of applications withdrawn and refused. However, even if all applications in this group were refused, the percentage of refusal is still very low, peaking in 2003/4 at one per cent.

There are mechanisms which could be incorporated into the legislative scheme at the point of issuing warrants which would allow for a stronger recognition of privacy interests. In Queensland, a PIM has the role of appearing at the hearing of applications for surveillance device warrants to examine witnesses and make submissions on the appropriateness of granting the application.[118] In its submissions to the Senate Committee, Electronic Frontiers Australia suggested that a public interest monitor be incorporated into the legislative scheme. During the course of the Senate debate, the Democrats suggested that a public interest monitor, based upon the Queensland model, be incorporated. However, no amendment

[118] *Queensland Police Powers and Responsibilities Act 1997* (Qld) s 159.

was pressed.

Secondly, the involvement of judicial officers is often seen as central to the warrant process, but the judicial involvement is increasingly being marginalised. As noted, there is no judicial involvement in Part 2.2 warrants. But, even in relation to Part 2.5 warrants, judicial involvement is increasingly more limited for two reasons: first, Federal Court judges have been reluctant to participate in the process and, secondly, the overwhelming number of applications is now made to AAT members.

In relation to the first, there has been a general retreat from the warrant process by Federal Court of Australia judges since the High Court's decision in *Grollo v Palmer*.[119] The Court in that case considered whether the function of issuing a warrant was compatible with the constitutional scheme of separating powers among three arms of government: the legislature, the executive and the judiciary. It is well established constitutional doctrine, that federal courts created by Parliament are only able to exercise judicial power or non-judicial power that is incidental to the exercise of judicial power.[120] The High Court held that the issuing of an interception warrant is an exercise of executive, not judicial, power. However, with considerable judicial ingenuity, the Court cleared the way for federal court judges to issue warrants if: (i) the power is conferred on the judge in his or her personal capacity (i.e., as *persona designata*); (ii) the function is not incompatible with the capacity of the judge or the court to exercise judicial power; and (iii) the judge consents to the exercise of the power. In holding that the power to issue interception warrants was not incompatible with the exercise of judicial power, a majority of the High Court emphasised the desirability of having judicial supervision of the process:

> Yet it is precisely because of the intrusive and clandestine nature of interception warrants and the necessity to use them in today's continuing battle against serious crime that some impartial authority, accustomed to the dispassionate assessment of evidence and sensitive to the common law's protection of privacy and property (both

[119] (1995) 184 CLR 348.

[120] *R v Kirby; ex Parte Boilermakers' Society of Australia (Boilermakers' Case)* (1956) 94 CLR 254.

real and personal), be authorised to control the official interception of communication.[121]

It was, the majority said, the 'professional experience and cast of mind of a judge'[122] that would guarantee an appropriate balance between law enforcement agencies and the person of interest. This, however, was not a view shared by all judges. McHugh J considered that 'public perception [of judges] must be diminished when the judges … are involved in secret, *ex parte* administrative procedures, forming part of the criminal investigative process, that are carried out as a routine part of their daily work.'[123]

In 1998, a number of judges of the Federal Court of Australia and the Family Court of Australia notified the Attorney-General that they would cease to participate in the granting of warrants under the legislation.[124] Consequently, Parliament amended the TI Act to allow AAT members to issue warrants. The most recent numbers show that Family Court judges and Federal Magistrates are still formally available to issue warrants (see Table 2), but only three Federal Court judges were formally available in the 2003/04 period.[125]

Table 2 – Availability of Federal Court Judges, Family Court Judges, Nominated AAT Members and Federal Magistrates to Issue

[121] *Grollo v Palmer* (1995) 184 CLR 348, 367 (Brennan CJ, Deane, Dawson and Toohey JJ).

[122] Ibid 367.

[123] Ibid 380. It was submitted to the Senate Committee that there may be some constitutional questions over the warrant provisions for stored communications because of the 'significantly more lenient' preconditions for exercising the power and the 'considerably less burdensome' reporting requirements: see Submission to Senate Legal and Constitutional Legislation Committee, Parliament of Australia, Canberra, 13 March 2006 (Gilbert & Tobin Centre of Public Law) 4. The central principle for determining validity in this context is whether the judge retains impartiality and independence from the other arms of government and the relevant court can be said to retain institutional integrity. This has been emphasised by the Court more recently in a context where similar principles are applied (*Fardon v Attorney General for the State of Queensland* (2004) 210 ALR 50). There does not appear to be anything in the legislative changes that threatens impartiality or integrity to any greater extent than the provisions before the Court in *Grollo*. If a future Court were to invalidate the provisions, it would be because it has adopted a different approach to that adopted in *Grollo*.

[124] *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004,* para 4.45.

[125] These figures, however, may not be a true reflection of the actual number of judges who are prepared to participate as many of them have not formally withdrawn their consent to issue warrants: ibid.

Warrants (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004,* Table 30).

ISSUER	NUMBER ELIGIBLE
NOMINATED AAT MEMBERS	18
FAMILY COURT JUDGES	21
FEDERAL COURT JUDGES	3
FEDERAL MAGISTRATES	16

The second reason why judicial involvement with the warrant process is more limited is because law enforcement agencies are seeking warrants primarily from AAT members. In the 2003/4 period AAT members issued 76 per cent of the warrants issued (see Table 3). This figure was even greater in the 2002/3 period, when 91 per cent of warrants were issued by AAT members. The increased use of AAT members to issue warrants was noted by the NSW Council of Civil Liberties to the Senate Committee.[126] Although the Committee was careful not to make any negative observations about the role of AAT members in the process, it recommended that a future review of the legislation 'should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime'.[127] The Democrats put forward a stronger position during the

[126] See Senate Legal and Constitutional Legislation Committee, above n 8, para 3.55.

[127] Senate Legal and Constitutional Legislation Committee, above n 8, Rec 25, para 4.112. This recommendation was supported by the Supplementary Report of the Democrats.

Senate debates, saying that they did not support having the AAT as an issuing authority: '[w]e believe, not only from looking at the statistics, that it is lowering a threshold. It is making it easier for warrants to be issued or obtained.'[128] The fact that AAT members have, at least on one occasion, met with law enforcement agencies to discuss 'generic issues'[129] tends to give the impression that AAT members do not see themselves as part of the checks and balances on law enforcement.

Thus, the reality of the warrant system does not reflect the perception: the percentage of warrant cases involving the involvement of judges is now significantly reduced.

Table 3 – Number of Warrants Issued in 2003-2004 Reporting Year by Federal Court Judges, Family Court Judges, Nominated AAT Members and Federal Magistrates (information taken from the *Telecommunications (Interception) Act 1979: Report for the Year ending 30 June 2004,* Table 31).

AGENCY	ISSUER			
	FAMILY COURT JUDGES	**FEDERAL COURT JUDGES**	**NOMINATED AAT MEMBERS**	**FEDERAL MAGISTRATES**
AUSTRALIAN FEDERAL POLICE	9	29	592	30
INDEPENDENT COMMISSION AGAINST CORRUPTION	0	0	31	0
AUSTRALIAN CRIME COMMISSION	0	11	379	0
NEW SOUTH WALES CRIME COMMISSION	0	0	824	0
NEW SOUTH WALES POLICE	0	0	6	457

[128] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 37.

[129] Sherman, above n 100, 11.

POLICE INTEGRITY COMMISSION	0	0	55	7
SOUTH AUSTRALIA POLICE	0	13	113	0
VICTORIA POLICE	0	0	269	0
WESTERN AUSTRALIAN ANTI-CORRUPTION COMMISSION	18	0	0	0
WESTERN AUSTRALIAN CORRUPTION AND CRIME COMMISSION	7	0	0	0
WESTERN AUSTRALIA POLICE	145	0	33	0
TOTAL	**179**	**53**	**2302**	**494**

4.5 Civil remedies

Part 2-10 of the TIA Act creates a civil remedy in favour of an aggrieved person in circumstances where there has been an interception in contravention of s 7(1), or a communication of information in breach of s 63. An individual is an 'aggrieved person' for these purposes if the person was a party to the intercepted communication or the communication was made on the person's behalf (s 107A). An application for such a remedy may be made to the Federal Court of Australia or a court of a State or Territory, or to a criminal court that has convicted a person of a breach of ss 7(1) or 63. The new Part 3-7 creates an identical mechanism for civil remedy in relation to the accessing of a stored communication in contravention of s 108(1), or the communication of information in contravention of s 133.

It is one thing for a civil remedy to be created, it is quite another for it to

be effective. The covert nature of the process of applying for a warrant will mean that it is only when the information becomes public, for example through a prosecution or enforcement process, that a person may become aware that he or she is an aggrieved person. Thus, innocent persons whose communications have been intercepted or accessed in contravention of the Act, and who are not later the subject of criminal prosecution or another enforcement mechanism, are unlikely to know whether they were aggrieved persons and entitled to a remedy under the Act. This issue surfaced during the Senate Committee inquiry, particularly in relation to B-Party warrants. The very nature of the B-Party warrant is that the subject of the warrant is likely to be an innocent party who may never be informed of an interception. The lack of such knowledge greatly reduces the effectiveness of the remedy. The point was made during the course of the Senate Committee hearings, in the context of a discussion of the possibility of seeking a review by the Ombudsman or the Inspector-General of Intelligence and Security ('IGIS') of an interception. In its Report, the Senate Committee said:

> It is theoretically open to any person adversely affected by the B-party warrant provisions to notify the Ombudsman, in the case of an agency, or the IGIS in the case of an ASIO warrant. However, the nature of the provisions and the covert nature of the surveillance makes it most unlikely if not impossible for such notification to occur. As the Committee Chair noted in the public hearing:
>
> > I am not entirely persuaded that one can complain to the Ombudsman or the IGIS about a telephone intercept that one does not know about.[130]

These comments are equally applicable to the likelihood of seeking a civil remedy. As Senator Stott Despoja said during the Senate Debate:

> Similar to stored communication warrants, we believe the ability of an aggrieved person affected by a B-party warrant to access civil remedies under the Telecommunications Act is ineffective.

[130] Senate Legal and Constitutional Legislation Committee, above n 8, para 4.101.

> Where a person has their communications unlawfully invaded or where material used from that interception is unlawfully recorded, they have no ability to seek redress because they will be completely unaware that the warrant has been exercised.[131]

In 1994, a review by Pat Barrett into the long term cost effectiveness of telecommunications interception recommended that 'agencies should be required to notify any innocent person whose telephone service has been intercepted of the fact of interception within a period of 90 days of cessation of the interception.'[132] As Barrett noted, there are notification mechanisms in the United States and Canada. Barrett's recommendation was not implemented by the government, but was raised again in a number of submissions to the Senate Committee.[133] Following the Democrats' unsuccessful attempt to introduce an amendment in the Senate, which would have required notification of a warrant in the case of stored communications warrants and B-Party warrants, the following exchange took place between Senator Ellison and Senator Stott Despoja as to the operation of the civil remedy provisions:

> Senator Ellison: … If there was a warrant executed which involved a B party and nothing was ever done in relation to the information concerning the B party, where would the harm be to the B party? You would have harm only if there were some action taken or they were prejudiced in some fashion. There would be a possibility of that occurring if you were to have proceedings in a court and that was all brought out. But, otherwise, it would never be acted upon. It could remain something which was of no consequence. …[134]

> Senator Stott Despoja: I am not talking about harm. The bill

[131] Commonwealth of Australia, *Parliamentary Debates,* Senate, 28 March 2006, 87-88. The Senator had earlier said that she thought it 'a little amusing that the government has included in the bill a section for civil remedies when the entire operation of the warrant is covert': at 86.

[132] Pat Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (1994) Rec 7, para 4.32.

[133] Electronic Frontiers Australia, above n 17, para 94; Australian Privacy Foundation, above n 26, para 18.

[134] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 18.

> provides for civil remedies if there is an aggrieved person. I am wondering how that person finds out that they are aggrieved or that some harm has been done to them. What I am tackling in this amendment is the issue of notification that a warrant has been issued. …[135]
>
> Senator Ellison: Under our law, any action has to be based on a case which demonstrates some disadvantage or harm. If a person never knows that they have been discriminated against – and this is across the board – they cannot bring the action.[136]

Senator Ellison's response that knowledge of harm is necessary for an action to be brought is self-evident, but it really misses the point. The TIA creates a civil remedy in circumstances where there has been an interception or access, or subsequent communication, in contravention of the statutory prohibitions. It is not a question of what harm may result once the information is publicly revealed as the Senator seemed to suggest. The relevant harm giving rise to the statutory claim is the unlawful interception or access or subsequent communication. If an aggrieved party is unaware of the circumstances giving rise to the remedy, then it is an ineffective one. The responses by Senator Ellison suggest either that, in the condensed period for debate, the Senator misunderstood the nature of the civil remedy provisions under the Act, or that the importance of maintaining the covert nature of the warrant process for security and law enforcement purposes outweighs the provision of an effective remedy to an aggrieved person. The second explanation is more likely. As the Senator said in one of his replies to Senator Stott Despoja, '[t]he fact is that if you notify people that you have a warrant against them you will destroy the whole regime this legislation is creating'.[137]

[135] Ibid.

[136] Ibid 19. The debate continued in similar terms over three pages of the Senate Hansard: at 18-20.

[137] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 March 2006, 20.

4.6 Enhancing security and law enforcement tools but leaving privacy protection behind

The 2006 amendments were described by the Attorney-General as 'enhanc[ing] interception powers and privacy protections'.[138] The changes, it was said, were designed to keep pace with technological change and 'ensure law enforcement and security have the investigative tools to continue to fight against serious crime and terrorist activity'.[139] While the amendments do enhance interception powers, they do not, to any significant degree, enhance privacy protections.

On the contrary, as the discussion in Part 2 demonstrates, at every point that a policy choice was to be made between security and law enforcement, on the one hand, and privacy, on the other, the government chose to sacrifice privacy interests. When introducing device warrants, it was recognised that technology would need to be developed before it confidently could be said that privacy interests of non-suspects would not be affected. Nevertheless, it was accepted by the Senate Committee that operational requirements of law enforcement and security warranted the amendment. The B-Party amendments were recognised during the Senate Committee process as impacting significantly on the privacy interests of innocent third parties. Opposition and Democrat amendments designed to limit the extent of the privacy intrusions were not accepted by the government. The broader stored communications scheme with relaxed thresholds was justified on a contested distinction between real-time and stored communications. Opposition and Democrat amendments designed to restore parity of privacy protection were not supported by the government. The relaxed reporting requirements in relation to stored communications were defended by the government from amendment on the basis that more detailed reporting would have an 'operational impact' on law enforcement objectives. The concern expressed by the Ombudsman about the capacity of his office to inspect and report under the stored communications scheme within the prescribed period was not seen as a 'compelling reason' to extend those

[138] The Hon Philip Ruddock MP, *Enhanced Interception Powers and Privacy Protections*, (Press Release, 30 March 2006)

[139] Ibid.

periods.

On the face of the amendments, the only significant measure designed to enhance privacy was the removal of the distinction between Class 1 and Class 2 offences and, consequently, the requirement that authorities issuing Part 2.5 warrants take account of privacy interests in all cases. However, as the Blunn Report recognised, where law enforcement needs are shown, privacy considerations are unlikely to preclude the issue of a warrant for any of the offences previously described as Class 1. Thus, in operation, the amendment is likely to have a minimal impact on privacy protection.

The government consistently maintained that the Blunn Report and Senate Committee recommendations would be the subject of ongoing consideration to ensure that the regime 'continues to achieve an appropriate balance between privacy and appropriate access for investigation of serious criminal conduct'.[140] The 2006 amendments, however, reinforce our previously stated concern that the regulatory landscape has changed to such an extent that 'there is no longer a position that resembles a "balance".'[141] Even if the 'balancing' metaphor is adopted, there would need to be substantial amendments to the legislative scheme to take account, at the very least, of the privacy concerns set out by the Senate Committee.

5 Concluding observations

The TIA Act was originally designed to protect wire-based national telecommunications infrastructure from unauthorised interception and to ensure access for national security and law enforcement purposes. However, the legislative assumptions and regulatory context have significantly changed since its original enactment. Changes in technology and patterns of criminal activity, and the increased attention on national security, have all placed pressure on government to provide enhanced legislative tools for national security and law enforcement. When these

[140] Ibid.

[141] S Bronitt and J Stellios, above n 42, 887

pressures are combined with the reduced judicial involvement in the warrant process and the largely illusory operation of the civil remedy provisions, the impact on privacy has been substantial.

These privacy implications are not merely the product of academic interest. Many of the fundamental privacy concerns were clearly expressed in the Blunn Report and the bipartisan report of the Senate Committee. The government has committed to reviewing their recommendations as part of an ongoing review of the legislation. We would renew our 'call for legislative reform that places rights protection at the centre of regulatory design',[142] but the implementation of the Senate Committee recommendations would be a useful start.

9

The application of critical social theory to national security research

Holly Tootell

School of Information Technology and Computer Science, University of Wollongong

Abstract

Current and proposed high-tech solutions to national security, specifically the use of

[142] Ibid 888.

Location-Based Services (LBS), are attracting increased attention from citizens as they become more pervasive. The connection between LBS and national security has been made in previous ICT studies but has been limited to either the technological or the privacy impact of LBS. They have not addressed the use of LBS from a 'lifeworld' perspective. To do this Habermas's Critical Social Theory (CST) is proposed as a method suitable for investigating the social impact of the technologies and identifying the factors driving governments to adopt such technologies. The theory is applied to the national security context.

Keywords: national security, critical social theory, location-based services, information systems research, content analysis

1 Introduction

This study seeks to examine the relationship that exists between the use of location-based services (LBS) and national security initiatives, and specifically the perceived impact they have on citizens.

Public awareness of national security has increased significantly since the terrorist attacks in the United States of America on September 11, 2001. Of the many high-technology solutions used in response to breaches of national security the use of complex information technologies, including radio frequency identification (RFID), global positioning system (GPS), and biometric identification appear to be the most popular. Location-based services require these technologies to provide functions that include: immigration and visa control applications (through biometric identification on passports) to advanced home-detention functionality (RFID chips for movement tracking), (James, 2004). Location applications have the potential to be privacy insensitive and pervasive, and are already considered by some to be inherently so (Adusei, Kyamakya et al., 2004 p.4). Evidence suggests that there is a need to research the impact that location applications have on society as a whole.

Previous studies of LBS with respect to national security have focused on two main categories: technology responses to resolving weaknesses in national security preparedness and communications; and privacy-based research that examine the responses of the public to the impact the proposed technologies will have on personal privacy. Although when drawn together these two perspectives create a relatively complete

picture of their use, lacking are the motivations and public reactions to the technologies that have been adopted.

To understand the motivations of government and drivers for public motivation and adoption, Critical Social Theory (CST) developed by Jurgen Habermas (1979; 1984) is applied. The primary objective of CST, and more particularly the application of CST to Information Systems (IS) research is to discover how "…many small IT changes add up to a policy that affects the nature of the society in which we live" (Klein and Huynh, 2004 p.157). CST's primary aim is emancipation through knowledge and study of past behaviour. CST allows the issue of LBS adoption for national security to be studied by examining events of national security significance through public reaction as documented in popular media.

For future advancement of government-driven solutions to national security threats and preparations, it is imperative that current research looks beyond the solutions themselves and develop greater awareness of their implications. The outcome of this research is to provide a framework for evaluating the impact of location-based solutions to national security problems and not to limit the development of technology or to prevent its use.

2 Location-based services for national security

Location-based services (LBS) exploit knowledge about where an information device is located. The information device can be used to locate living and non-living entities (people, artefacts in rooms, etc.). Location can be represented in a variety of ways e.g. address or latitude/longitude. Depending on the context LBS can utilize several technologies for knowing where an information device is geographically located. Global positioning system (GPS), cell identification, broadband satellite network, assisted GPS, wireless local area networks (WLAN) and radio frequency identification (RFID) are examples of technologies used (Rao and Minakakis, 2003).

LBS are used in multiple market segments: personal, commercial and government, for diverse purposes, including navigation and personalized marketing material dependent on location. LBS also provide a technological solution to the more serious issue of national security. Their

ability to calculate position information (either push or pull in nature) provides an invaluable resource for preventive, protective and responsive situations. A *pull* technology requires the user to request the information, where a *push* service delivers the information automatically based on the position of the user. An example of the LBS technologies being used in national security include: RFID for disaster management, disease outbreaks, and secure access control; GPS devices for monitoring emergency response teams and the monitoring of public health outbreaks and mobile stations for emergency response.

3 Critical social theory in information systems research

Qualitative research is used when the focus of research is the “real world” (Leedy, 2005 p.133). The tools of qualitative research allow a researcher to interact with those the research phenomenon effects, both directly and through social artefacts like newspapers, popular magazines and other feedback sources (Leedy, 2005 p.144). A qualitative approach is most useful when a researcher wants to describe, interpret, verify or evaluate the impact of a particular area of interest (Leedy, 2005 p.134).

Critical Social Theory (CST) is a qualitative approach to research. There are three underlying paradigms in which qualitative research can take place: positivism, interpretivism and critical theory. Positivism and interpretivism are the two most common approaches used by researchers in Information Systems (Orlikowski and Baroudi, 1991), however over the past twenty years there has been a significant body of work that has been applying critical theory to Information Systems research topics (Cecez-Kecmanovic, 2001b; Cecez-Kecmanovic, Janson et al., 2002).

The critical approach differs from interpretivist in that it seeks to understand the workings of the whole phenomena: a critical study in Information Systems cannot look at technology alone, it must strive to understand it in terms of the industrial, societal and national context it is applied in (Myers, 1997; Orlikowski and Baroudi, 2002). It is the impact that innovation has had on the population that is most critical to its success or failure. A critical researcher aims to better understand how societies work to produce beneficial and detrimental effects, in this case through adoption of location applications. The researcher then looks for

ways to mitigate or eliminate the damaging effects (of the location applications) (Fairclough, 2003). Critical researchers use knowledge that is grounded in social and political practices. Historical analysis of a phenomena is used to identify long-held associations (Orlikowski and Baroudi, 2002). McGrath (2005) states that "[f]or more than 30 years, critical research in information systems (IS) has challenged the assumption that technology innovation is inherently desirable and hence to the benefit of all." Cezec-Kemanovic (2001a; 2002), Kirkpatrick (2004), Lyytinen and Klein (1985), Lyytenin and Ngwenyama (1992), Ngwenyama and Lee (1997) and Wong (2004) are researchers who have investigated and applied the work to IS research. It is a method designed to reveal "hidden agendas, concealed inequalities and tacit manipulation" in the examination of the complex relationships of information systems, socio-political and organisational contexts (Cecez-Kecmanovic, 2001b). CST is a qualitative approach to Information Systems (IS) research. It differs from an interpretivist perspective by its intention to emancipate the subjects of the study, rather than to empathise with them. Figure 1 describes the relationships between approaches to IS research and a suggestion of tools used to operationalise the theories.

Where interpretive researchers seek to maintain the *status quo* (Walsham, 2005), critical researchers seek to emancipate subjects. Habermas' theory is intent on effecting radical change through understanding distortions of communications (Cukier, Bauer et al., 2004). CST looks to the outside world and examines opinions that appear in the 'public sphere', defined by Fairclough as the connection between social systems and the domain of everyday living ("lifeworld"), where people deliberate on matters of social and political concerns (Fairclough, 2003). Lifeworld is a term used by Habermas to refer to a common world of experience (Habermas, 1984). Cecez-Kecmanovic (2001b) describes it as the 'taken-for-granted' universe of daily social activities of members'. CST implies that the researcher has an agenda and is setting out to examine the 'lifeworld' to come to understand the meaning of things.

Lyytinen and Klein (1985 p.219) state: *"[Habermas' critical theory] suggests that information systems which are designed to increase organisational effectiveness must also increase human understanding and emancipate people from undesirable social and physical constraints,*

distorted communication and misapplied power." The questioning of the neutrality of technology is essential to understand the social impact of new schemes. Particularly in critical IS research, the aim is to expose attempts to "design and (mis)use IS to deceive, manipulate, exploit, dominate and disempower people." (Cecez-Kecmanovic, 2001b).

Figure 1: Methodological Approach-
adapted from Titscher (2000 p.51) and Cecez-Kecmanovic (2001b p.150)

4 National security and critical social theory

The "primary objective of CST is the improvement of the human condition" (Ngwenyama, 1991). A number of technology studies have researched the importance of wireless services in disaster recovery efforts (Balachandran, Budka et al., 2004; Malone, 2004), particularly the uptake of commercial network provision as a viable alternative for the small market of public safety. They have identified that if primary communications infrastructure is damaged or destroyed, it is the mobile services that are the lifeline. Connolly (2003), Chen (2004) and Popp (2004) (2004) identify the significance that IP location and internet content can make in making knowledge links for counter-terrorism responses. In each of these studies, a particular application of the technology is examined, which allows for an in-depth understanding of the system to occur, but for disaster planning, it does not provide an over-arching view of the technology solutions being used together. Nor does it examine the impact these technologies can have when applied outside the realm of national security application.

Privacy studies have identified LBS technologies as being perceived as a threat to privacy regardless of purpose (Strickland and Hunt, 2005). They have also examined the change in public perception to information collection and management for the purpose of 'homeland' security (Meeks, 2003; Feinberg, 2004). Halchin (2002; 2004) has examined the use of government websites by terrorist organizations as an aid to planning attacks. From this aspect, control and management of

information is seen as critical to the fight to protect national security. However the counter argument to this is that by restricting access to online government information, potential terrorists are prevented from getting access, as are ordinary citizens.

Seifert (2002; 2004) has written about the importance of information storage and collections in terms of infrastructure management, related to this is the research by Raghu (2003) that examines the need for collaborative decision making. This approach to national security research, although not from a technical or LBS perspective, is at least beginning to examine the problem holistically.

The use of CST will allow the researcher to investigate the impact location applications for national security has through public perception. The content analysis tool nVivo will be used to investigate the phenomenon through popular media sources. The content to be analysed can include words, phrases, sentences, paragraphs, pictures, symbols, or ideas (O'Connor, 2004). Content analysis has gained momentum as a research method through the rapid expansion of mass communication, both mass media and international politics (Titscher, Meyer et al., 2000). Content analysis is useful for making inferences by objectively and systematically recognizing particular patterns within messages and it does not need to be limited to textual analysis (Holsti, 1969).

Throughout this data collection and analysis, the researcher will be looking for indications of change in government perspective and response to events of interest, also for changes in public sentiment with regard to proposed solutions. Anecdotal evidence suggests that at selected time periods after an event of national security significance, public sentiment changes to reflect a more learned appreciation of measures that have taken place in response to the event. Through performing multiple analyses of the same data sets but focusing on specific indicators eg: event, time period, or technology, indicators of change will be able to be extracted and compared.

5 Conclusion

Whether it is the use of RFID bracelets to monitor home-detention prisoners, the implementation of biometric identification passport systems

or the development of GPS monitoring systems for natural disaster management, the notion that personal privacy will be affected in order to enhance security cannot be denied. Previous studies have primarily focused on the implementation of a single LBS or the privacy impact of one location technology. From this it has been difficult to identify the continual shift in public perception and reaction to LBS. To determine the wide-ranging effects of the application of LBS to national security, the focus provided by CST, combined with the results of the content analysis, will bring together a detailed study of the concept of privacy and civil liberties being exchanged for security.

References

Adusei, I. K., K. Kyamakya, et al. (2004). “Location-based services: advances and challenges.” Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513). IEEE. Part Vol.1, 2004: 1-7 Vol.

Balachandran, K., K. C. Budka, et al. (2004). “Third-generation wireless services for Homeland Security.” Bell Labs Technical Journal **9**(2): 5-21.

Cecez-Kecmanovic, D. (2001a). Critical Information Systems Research: A Habermasian Approach. The 9th European Conference on Information Systems, Bled, Slovenia.

Cecez-Kecmanovic, D. (2001b). Doing Critical IS Research: The Question of Methodology. Qualitative Research in Information Systems: Issues and Trends. E. Trauth. Hearshy, PA., Idea Group Publishing**:** 141 - 163.

Cecez-Kecmanovic, D., M. Janson, et al. (2002). “The rationality framework for a critical study of information systems.” Journal of Information Technology **17**(4): 215.

Chen, H., F.-Y. Wang, et al. (2004). “Intelligence and security informatics for homeland security: information, communication, and transportation.” Intelligent Transportation Systems, IEEE Transactions on **5**(4): 329-341.

Connolly, G., A. Sachenko, et al. (2003). Distributed traceroute approach to geographically locating IP devices. Intelligent Data Acquisition

and Advanced Computing Systems: Technology and Applications, 2003. Proceedings of the Second IEEE International Workshop on.

Cukier, W., R. Bauer, et al. (2004). Applying Habermas' Validity Claims as a Standard for Critical Discourse Analysis. Information Systems Research: Relevant Theory and Informed Practice. B. Kaplan, D. P. Truex III, D. Wastell, A. T. Wood-Harper and J. I. DeGross. Massachusetts, Kluwer Academic Publishers**:** 233 - 258.

Fairclough, N. (2003). Analysing Discourse: Textual analysis for social research. London, Routledge.

Feinberg, L. E. (2004). "FOIA, federal information policy, and information availability in a post-9/11 world." Government Information Quarterly **21**(4): 439-460.

Habermas, J. (1979). Communication and the evolution of society / Jurgen Habermas; translated and with an introduction by Thomas McCarthy. London:, Heinemann,.

Habermas, J. (1984). The theory of communicative action. Boston:, Beacon Press,.

Halchin, L. E. (2002). "Electronic government in the age of terrorism." Government Information Quarterly **19**(3): 243-254.

Halchin, L. E. (2004). "Electronic government: Government capability and terrorist resource." Government Information Quarterly **21**(4): 406-419.

Holsti, O. R. (1969). Content analysis for the social sciences and humanities / Ole R. Holsti. Reading, Massachusetts, Addison-Wesley.

James, M. (2004). "Where are you now? Location detection systems and personal privacy." Science, Technology, Environment and Resources Section Research Note no. 60 2003–04. Retrieved 30 May, 2005, from http://www.aph.gov.au/library/pubs/rn/2003-04/04rn60.htm.

Klein, H. K. and M. Q. Huynh (2004). The Critical Social Theory of Jurgen Habermas and its Implications for IS Research. Social Theory and Philosophy for Information Systems. J. Mingers and L. Willcocks. West Sussex, England, John Wiley & Sons Ltd.**:** 157 - 237.

Leedy, P. D. (2005). Practical Research: Planning and Design. New Jersey, Prentice Hall.

Lubick, N. (2004). “Homeland security and geospatial data.” Geotimes **49**(7): 11-13.

Lyytinen, K. and H. K. Klein (1985). The Critical Theory of Jurgen Habermas as a basis for a Theory of Information Systems. Research Methods in Information Systems. E. Mumford. North-Holland, Elsevier Science Publishers**:** 219-236.

Lyytinen, K. J. and O. K. Ngwenyama (1992). “What does computer support for cooperative work mean? a structurational analysis of computer supported cooperative work.” Accounting, Management and Information Technologies **2**(1): 19-37.

Malone, B. L. (2004). “Wireless search and rescue: Concepts for improved capabilities.” Bell Labs Technical Journal **9**(2): 37-49.

McGrath, K. (2005). “Doing critical research in information systems: a case of theory and practice not informing each other.” Information Systems Journal **15**(2): 85-101.

Meeks, B. N. (2003). “Conspicuous in their silence - Where are the voices defending the very fought-after privacy rights now threatened in the name of Homeland Security?” Communications of the ACM **46**(2): 15-16.

Myers, M. D. (1997). “Qualitative research in information systems.” MIS Quarterly **21**(2): 241.

Ngwenyama, O. K. (1991). The Critical Social Theory approach to Information Systems: Problems and Challenges. Information Systems Research: Contemporary Approaches and Emergent Traditions. H. E. Nissen, H. K. Klein and R. Hirschheim. Amsterdam, North-Holland.

Ngwenyama, O. K. and A. S. Lee (1997). “Communication richness in electronic mail: Critical social theory and the contextuality of meaning.” MIS Quarterly **21**(2): 145.

O’Connor, T. (2004). “Research Methods.” from http://faculty.ncwc.edu/toconnor/308/default.htm.

Orlikowski, W. J. and J. J. Baroudi (1991). “Studying information technology in organizations: research approaches and assumptions.” Information Systems Research **2**: 1-28.

Orlikowski, W. J. and J. J. Baroudi (2002). Studying Information Technology in Organizations: Research Approaches and

Assumptions. Qualitative Research in Information Systems: A reader. M. D. Myers and D. Avison. London, SAGE Publications Ltd**:** 51 - 78.

Popp, R., T. Armour, et al. (2004). “Countering Terrorism through Information Technology.” Association for Computing Machinery. Communications of the ACM **47**(3): 36.

Raghu, T. S., R. Ramesh, et al. (2003). Addressing the homeland security problem: A collaborative decision-making framework. Intelligence and Security Informatics, Proceedings. **2665:** 249-265.

Rao, B. and L. Minakakis (2003). “Evolution of mobile location-based services.” Communications of the ACM **46**(12): 61-65.

Seifert, J. W. (2002). “The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned.” Government Information Quarterly **19**(3): 225-242.

Seifert, J. W. and H. C. Relyea (2004). “Do you know where your information is in the homeland security era?” Government Information Quarterly **21**(4): 399-405.

Strickland, L. S. and L. E. Hunt (2005). “Technology, security, and individual privacy: New tools, new threats, and new public perceptions.” Journal of the American Society for Information Science and Technology **56**(3): 221-234.

Titscher, S., M. Meyer, et al. (2000). Methods of Text and Discourse Analysis. London, SAGE Publications.

Walsham, G. (2005). “Learning about being critical.” Inform Syst J **15**(2): 111-117.

Wong, C. K. (2004). Making sense of even a technology change: an interpretive approach to IT implementation. Midwest Academy of Management, Minneapolis, Creighton University.

10

Australia's anti-terrorism legislation: the national security state and the community legal sector

Mark Rix

Graduate School of Business, University of Wollongong

Abstract

This paper considers the implications for the community legal sector of the Australian Government's recent national security and anti-terrorism legislation. Critics of the legislation have deep concerns that, by giving the police and intelligence services considerable new powers in the areas of arbitrary arrest and detention, it will lead to the significant erosion of rights and freedoms that Australians have been able to take for granted. Other concerns with the legislation relate to the use of force, sedition, and legal representation for those held in preventative detention. In addition, the legislation has no adequate protection against the intelligence services and police misusing or abusing their new, extended powers. Community legal centres (CLCs), that comprise the community legal sector, have the important role of informing citizens of their basic rights and assisting them in exercising these rights in their dealings with government and its agencies. This paper will consider what effects the anti-terrorism legislation will have on the community legal sector's effectiveness in playing this role. The sector, which the Australian government relies on and funds to provide legal services to some of the most disadvantaged members of the Australian community, has as its raison d'être improving

access to justice and equality before the law for all Australians. The paper will also consider the impact of the anti-terrorism legislation on the relationship between the government and the sector.

Keywords: anti-terrorism legislation, national security state, community legal sector, citizens

1 Introduction

This paper considers the implications of the Australian Government's recent national security and anti-terrorism legislation for the community legal sector. The legislation, in particular, The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 and the Anti-Terrorism Bill (No. 2) 2005 which passed through both houses of the Australian Parliament in December 2005, are without precedent in this country in that they respectively provide ASIO and the Australian Federal Police with the new power to detain those suspected of posing a terrorist risk to the community. Thus, they allow for detention without charge or trial. In other words, the authorities will have the power to detain a person they do not have sufficient evidence to charge with a criminal offence. The control order, preventative detention and sedition provisions of the 2005 Bill are also of great concern, allowing much scope for misuse and abuse by the authorities under the pretext of protecting Australia's national security. The paper will consider what impact this legislation will have on the community legal sector and its relationship with the Australian Government. The sector is funded by the Government to provide legal services to some of the most disadvantaged members of the Australian community, but has as its self-declared *raison d'être* the improvement of access to justice and equality before the law of all Australians. Thus, in informing and educating members of the Australian community about the provisions of the national security and anti-terrorism legislation the sector will run the risk of coming into conflict with the Government. This may put the sector in danger of funding cuts or other restrictions affecting its ability not only to provide assistance to the poor and disadvantaged but also of effectively performing its important community legal education role.

2 An Australian national security state?

Even a cursory visit to the Australian Government's national security website http://www.nationalsecurity.gov.au (hosted by the Attorney-General's Department) is an instructive, and unsettling, exercise. Some years ago Australians were urged by Prime Minister John Howard and his government to *be alert, but not alarmed* when coming to terms and preparing to deal with the threat of terrorist attack. This message was contained in a series of television advertisements that were screened following the Bali bombings of October 2002. However as Matt McDonald points out, the most important initiative of the Government's 'National Security Public Information Campaign' "was the anti-terrorism kit and specifically the *Let's Look out for Australia* booklet, which the government attempted to distribute to all Australian homes in February 2003" (McDonald 2005: 177). In any event, the vast quantities of alarming information available on the national security website suggest that the Government should soberly heed its own advice. For, the amount and type of information provided there give the distinct impression that the Government believes the terrorist threat to be so serious and imminent that the most effective way of dealing with it is to drastically curtail the rights and freedoms of the Australian people. Much of this information introduces and explains the extensive amounts of anti-terrorism legislation that has been passed into law over the past three years or so.

Four noteworthy aspects of this legislation are that it "(1) defines terrorism in sweeping terms; (2) permits the banning of political groups; (3) allows for detention without trial; and (4) shrouds the operations of the intelligence and security agencies in secrecy and provides for semi-secret trials" (Head 2005: 210). According to Christopher Michaelson, the anti-terrorism legislation is a "clear overreaction" to a terrorist threat that remains relatively minor. This is in spite of Australia's involvement in the invasion and occupation of Iraq, its continued military role in Afghanistan, and more generally its support for the global war on terrorism led by the United States. Such factors as Australia's geographical isolation, the border protection and immigration control system that it has put in place, and the absence of a "human infrastructure" capable of organising and mounting a major terrorist attack mean that there is only a low probability of such an attack occurring within Australia. Comments Michaelson,

“Many of the new laws are not only ill-conceived but also constitute a disproportionate legal response to the threat Australia is currently facing from international terrorism” (Michaelson 2005: 334).

Clicking on the legislation link on the national security website opens a chilling vista onto a truly remarkable collection of national security, in particular anti-terrorism, legislation that aims to deal with the threat of terrorist attack whether it is ‘home grown’ or foreign-based. The collection is an impressive tribute to the energy and determination of Australia’s law makers when it comes to what they obviously regard as their chief responsibility and highest public duty, namely, tightening Australia’s ‘national security’ system thus protecting the country and the Australian people from terrorism. The notion that there might be other, equally or more pressing priorities to which the law makers should urgently be directing their energies to improve national security, such as the chronic problems with the health system, a massively under-funded tertiary education sector, an often dysfunctional justice system, to name just a few, seems to have been largely overlooked by them. Similarly, that the terrorist threat may not be quite as imminent or massive as suggested by the legislative onslaught is evidently not to be taken as a serious proposition.

3 Australia’s anti-terrorism laws

In the section headed ‘Australian Laws to Combat Terrorism’ on the legislation link, it is stated that “Australia has long played a leading role in the development of laws to combat terrorism”, the Australian government having introduced “an extensive legislative regime around counter-terrorism, national security and other cross-jurisdictional offences” (‘Australian Laws to Combat Terrorism’ n.d.). This could be something of an understatement, because it is also made clear that the many acts listed are only “key pieces” of national security and anti-terrorism legislation. Not only has legislation such as the Crimes Act 1914 recently been amended to render it more effective in dealing with terrorist threats, “new legislation has been enacted to ensure Australia and Australians are protected from *emerging threats*” (‘Australian Laws to Combat Terrorism’ n.d.; emphasis added). The following brief review of

Australia's anti-terrorism laws does not investigate the entire "extensive legislative regime" in detail. Instead, it selects for discussion and analysis those acts that are most representative of the worrying tendency of the Federal Government to trample on the rights and liberties of Australian citizens in the name of protecting the country's national security.

The Anti-Terrorism Act 2004, for example, amongst other things amends the crimes Act 1914 "to strengthen the powers of Australia's law enforcement authorities, setting minimum non-parole periods for terrorism offences and tightening bail conditions for those charged with terrorism offences" ('Australian Laws to Combat Terrorism' n.d.). It introduces the new offence of training with a terrorist organisation that has been proscribed, an offence that carries a maximum penalty of 25 years imprisonment. The Anti-Terrorism Act (No. 2) 2004 amends the Criminal Code Act of 1995 making it an offence "to intentionally associate" with someone who is a member of a listed terrorist organisation. It thus builds on the provisions of the Security Legislation Amendment (Terrorism) Act 2002 which is analysed below. For its part, The Anti-Terrorism Act (No. 3) 2004 amends the Passports Act 1938, the Australian Intelligence Security Act 1979 and the Crimes Act 1914 with a view to improving the Australian legal framework relating to counter-terrorism ('Australian Laws to Combat Terrorism' n.d.).

The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 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 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. Michaelson concludes that “In effect, these provisions abandon several fundamental principles of the rule of law: they dilute the prohibition of arbitrary detention, they obliterate the right to habeas corpus, they remove the right to silence, and they reverse the onus of proof” (Michaelson 2005a: 178).

The Security Legislation Amendment (Terrorism) Act 2002 amends the Criminal Code Act 1995 thereby modernising treason offences and creating new terrorism offences and offences relating to “membership or other specified links to terrorist organisations” (‘Australian Laws to Combat Terrorism’ n.d.). In amending the Commonwealth Criminal Code, the Act creates the offence of associating with a terrorist organisation. Power is granted to the Governor-General (the executive branch of the Australian state) “to make regulations (delegated legislation) declaring an organisation to be a ‘terrorist organisation’” (Jackson 2005: 134). The Act defines a ‘terrorist act’ so broadly that it criminalises, and subjects to severe penalties, any actions taken in support of a political movement which engages in “physical resistance” against an existing government (in Australia or overseas). By denying Australians the right to associate with such movements, the Act “threatens to undermine the very democracy which these offences seek to protect” (Jackson 2005: 138).

The already much-amended Crimes Act 1914 is further amended by The Crimes Amendment Act 2005 with the effect of enabling participating Commonwealth agencies “to request assumed identity documents from State and Territory issuing agencies in accordance with legislation in force in those jurisdictions” (‘Australian Laws to Combat Terrorism’ n.d.). The National Security Information (Criminal Proceedings) Act 2004 was amended by the National Security Information Legislation Amendment Act 2005 to extend the protection from disclosure of “security sensitive information” by including “certain civil court proceedings” (Australian Laws to Combat Terrorism’ n.d.). The National Security Information (Criminal and Civil Proceedings) Act 2004 is the result. The amendments to the original national security information bill have only served to strengthen its provisions. As Patrick Emerton notes, “The purpose of the Bill… is to permit the prosecution and conviction of individuals on the

basis of information which, for reasons of national security, is not itself tendered in evidence against them at trial" (Emerton 2004: 143). Amongst other things, the Bill also allows for partially, or even completely, secret trials, evidence to be censored, and defendants and their lawyers to be excluded from trial proceedings (Head 2005: 211).

3.1 The Anti-Terrorism Bill (No. 2) 2005

Beneath the list of key pieces of Australian legislation to combat terrorism comes a disclaimer and stern warning: "Because the global security environment is dynamic, the Australian Government is continually responding to ensure our legislative regime is current, comprehensive and appropriate" such that "at any time, further initiatives may be under consideration by Parliament" ('Australian Laws to Combat Terrorism' n.d.). As it happens, one of the key, and certainly one of the most draconian, pieces of anti-terrorism legislation has only recently been included on the national security website.

On the evening of 6 December 2005 Coalition and Opposition (and Family First) Senators voted together to pass the Anti-Terrorism Bill (No. 2) 2005. This capitulation by the Opposition was hardly surprising given that on September 28, Labor leader Kim Beazley had announced that in the Opposition's view the new anti-terrorism laws proposed by the Government "did not go far enough" (Beazley quoted in Hocking 2005). Mr Beazley had also recommended even stronger powers "'allowing police to lock down entire suburbs and carry out house, vehicle and people searches without judicial approval'" (Beazley quoted in Nettheim 2005: 7). Greens and Democrat Senators voted against the Bill, but they were heavily outnumbered. In a Press Release announcing the passage of the Bill through both houses of the Australian Parliament, Attorney-General Philip Ruddock described it, and the measures it includes, as a "proportionate and appropriate response" to the terrorist threat facing Australia. According to Mr Ruddock, the new bill and related legislation "place Australia in a strong position to prevent new and emerging threats and to stop terrorists carrying out their intended acts" (Ruddock 2005a). The Bill's "key features" 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).

3.2 The 2005 Bill's preventative detention, control orders and sedition provisions

Unfortunately, the Attorney-General omitted from his Press Release important aspects of the "key features" that are rather more disquieting than his bland statement would suggest. For example, 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).

Prior to the passage of the Anti-Terrorism Bill (No. 2) 2005 through the Parliament, Mr Ruddock announced that the Government had accepted amendments suggested by the Senate Legal and Constitutional Legislation Committee and "other government members" (comprising a special backbench committee) that would "improve and strengthen" the Bill (Ruddock 2005). There is not the time or space here to run through all the amendments, but several of the most important will briefly be discussed.

The amendments to the Bill's preventative detention and control orders that were accepted by the Government will require anyone that is subject to a continuing order to be provided with a full statement of the allegations that led to the invoking of the orders in the first place.

However, for John North, President of the Law Council of Australia, these amendments would still not pass a crucial legal test. While the amendments would give a person subject to preventative detention and control orders the ability to repudiate the orders, because there is insufficient evidence to formally charge them with an offence they would not know precisely what they were opposing or challenging (North 2005). In other words, even with the amendments the inclusion of these orders in the Bill is tantamount to the legalisation and legitimisation of detention without evidence or trial. And in an important caveat, the provision allowing for a person subject to a control order to be informed of about why the restrictions were imposed "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 requirements applying to an AFP request for variation of a control order ('Details of Amendments'; attachment to Ruddock 2005).

Even though the Bill was subjected to sustained criticism from within and outside the Government (not including Opposition Leader Beazley) for its inclusion of a newly-defined crime of sedition, the sedition provisions were retained in a 'softened' form. The softening of these provisions makes it clear that a so-called seditious intention in essence involves the intention to use or threaten the use of force or violence to achieve a specified outcome. Another significant amendment removed the phrase "by any means whatsoever' in the offences of urging a person to assist the enemy and urging a person to assist those engaged in armed hostilities". The government also accepted an amendment allowing for an "additional good faith defence in relation to publishers of material who do so in good faith and in the public interest" ('Details of Amendments'; attachment to Ruddock 2005). Nevertheless, critics remain concerned that the crime of sedition is open to abuse and misuse by the Government just as it has been in other countries. In a lame concession to opponents of the Bill, Attorney-General Ruddock also announced that the crime of sedition would be subject to "detailed review".

4 Australian anti-terrorism legislation: what are the implications for the community legal sector?

In the following section, the implications for the community legal sector of Australia's anti-terrorism laws will be considered. This sector, which the Australian government relies on and funds to provide legal services to some of the most disadvantaged members of the Australian community, has as its *raison d'être* improving access to justice and equality before the law for all Australians. Thus, even though in providing legal services to disadvantaged individuals and groups the sector is acknowledged to be a key part of the Australian Government's social justice strategy, the sector often finds itself in conflict with the Government and its agencies when seeking to improve access to justice and equality before the law for its clients. The recently introduced anti-terrorism legislation is likely to mean that the conflict and tensions between the Government and sector will become more intense and difficult.

4.1 The community legal sector: roles and responsibilities

There are more than 200 community legal centres (CLCs) across Australia, 129 of which are funded under the Commonwealth Community Legal Services Program (CCLSP). Under this program, the sector is funded to provide legal services to "disadvantaged" members of the Australian community. The national data reporting system used by the Commonwealth-funded CLCs yields statistics which demonstrate the important role played by CLCs in the Australian community: "In the last 8 years, these 129 centres have provided services to more than 1.5 million people throughout Australia in urban, regional and remote areas, and provided over 2.5 million instances of legal advice, information and case assistance" (NACLC 2003: 11). In addition to their community legal education, law reform and policy activities, the 129 centres tallied an impressive 450,000 individual service interactions which included provision of legal advice and information and opening of new cases (Rix 2005).

4.2 The Commonwealth Community Legal Services Program

According to the CCLSP Program Guidelines, the Program is part of the Commonwealth's contribution to legal aid and forms "a vital part of the Commonwealth's multi-layered approach to addressing the legal needs of the disadvantaged members of the community" (AGD 2005). The CCLSP has a number of specific and significant objectives:

- Community legal services assist people, individually or collectively, as well as the community overall. Assistance is directed towards people who experience some form of systemic or socio-economic barrier to accessing legal services and/or whose interests should be pursued as a matter of public interest.
- Community legal service clients receive early assistance through the provision of appropriate information and referral.
- Community legal service clients gain a practical and improved understanding of legal and other options available to them through the provision of appropriate advice.
- Community legal service clients, through the provision of appropriate casework, gain an increased opportunity to pursue outcomes consistent with their legal rights or entitlements and community legal service resources (AGD 2005).

In addition, community legal centres undertake community legal education (CLE) and law reform and policy work. CLE is designed to provide individuals and groups, and other service providers and agencies, with information to improve their knowledge and understanding of the legal system. It is also meant to enhance people's ability to engage with the legal system and to use legal processes effectively. No less important, CLE activities inform people of the rights they have and educate them about how to exercise their rights. The law reform and policy work undertaken by CLCs is designed to enable them more effectively to meet the legal and related needs of the members of the communities they serve.

CLCs thus play an important role in maintaining social order and preventing social fragmentation. On this, the National Association of Community Legal Centres (NACLC) pointed out in a 2003 discussion paper that all Australian governments had failed to acknowledge just how important legal citizenship is in modern democracies like Australia's. In

essence, legal citizenship refers to the right of all citizens to have “fair and effective access to the justice system” (NACLC 2003). Legal citizenship requires governments to put in place policies and programmes enabling all citizens to give effect to this right. Legal citizenship is fundamental to the maintenance of social order and stability, and to the prevention of social fragmentation, for the idea that “each citizen is equal before the law and should have access to justice is essential to the community’s confidence and compliance with the law” (Federation of CLCs Vic 2003). Such confidence in and compliance with the law are absolutely essential because the law is what establishes “the shape of society and its character” (NACLC 2003).

Maintaining confidence in and compliance with the law has become an increasingly daunting challenge as the number of laws encroaching on citizens’ everyday life has proliferated making the justice system more complex and difficult to negotiate. NACLC estimates that, since the 1970s, there has been a doubling of legislation affecting the daily lives of citizens without any corresponding increase in resources and funding for legal advice, representation and community education. “Ordinary citizens”, observes NACLC, “are now expected to understand, interpret and negotiate the legal landscape alone in a climate of increasing complexity and reduced government commitment to civil society (NACLC 2003a).

4.3 The community legal sector: protecting Australia’s national security

In ensuring that people have confidence in the law so that they are willing to comply with it, and in this way preserving social order and peace and preventing social fragmentation, the community legal sector actually plays an important, but largely unheralded, role in protecting Australia’s national security. Indeed, its role in doing so is at least as important as the Government’s when, by enacting draconian anti-terrorism laws, it claims to be defending the national security of the country. The Government’s manifold anti-terror legislation joins the long list of laws affecting the daily lives of citizens that have been enacted over the past 30 years or so. The inclusion in the most recent piece of such legislation of detention and control orders and the crime of sedition, and associated severe restrictions on the disclosure of information, has

further increased the complexity of the justice system and made it even more difficult to negotiate successfully. This will have the effect of increasing the importance of the community legal sector's role in protecting the national security of Australia. For, the sector will with greater frequency and urgency be called upon to ensure that ordinary Australian citizens have access to justice and enjoy equality before the law in the face of the Australian Government's curtailment of these rights. This is a function that the sector will have to perform even while it continues to undertake the indispensable activities prescribed for it in the Community Legal Services Program Guidelines.

In meeting the challenges with which community legal sector will be confronted by the anti-terrorism legislation, the importance of the Community Legal Education work undertaken by the sector will become even more pronounced. The sector's CLE work will have to focus on the legislation that makes it possible for the authorities to detain people without trial. In this respect, the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 deserves special mention. Also deserving wide exposure and careful explanation are those aspects of the Anti-Terrorism Bill (No. 2) 2005 that make it possible for the Australian Federal Police and other national security authorities to use preventative detention and control orders for the detention of individuals without evidence or trial. As seen above, this in effect gives the authorities the ability to detain people even where there is insufficient evidence to charge them with a criminal offence. Thus, the authorities can hold people whom they suspect of posing a terrorist 'risk' to the community. Just as worrying are the Bill's provisions allowing the authorities to withhold information from a person subject to a control order when they believe that disclosure would, amongst other reasons, prejudice national security. The claim of protecting national security thus gives the authorities *carte blanche* to withhold information in any and all cases in which preventative and control orders are employed. For, the authorities' decision to do so could never be effectively challenged because the information that could provide the grounds for an appeal remains secret and hidden. It will be important for the community legal sector through its CLE activities to inform and educate members of Muslim communities and groups whose members are of Middle Eastern

origin, and other so-called ‘suspect’ groups, about the Bill’s provisions. After all, it is these communities and groups who are most at risk from the persecution, harassment and arbitrary detention permitted in the legislation under the pretext of preventing terrorism and protecting national security. As Luke Howie observes, “[a]s long as Australians victimise Muslims and allow latent xenophobic urges to surface, extremist attitudes will gain in popularity” (Howie 2005: 23).

It is not only the provisions allowing for preventative and control orders to be invoked by the authorities that will have to be emphasised in the sector’s CLE activities, the crime of sedition contained in the 2005 Bill also requires its implications to be highlighted and explained to members of suspect groups. The authorities have only to suspect a person of seditious intent to use, “urge” or threaten the use of force for them to be able to invoke the applicable provisions of the Bill. This ‘softening’ of the sedition provisions contained in an earlier draft of the Bill (which had referred simply to a “seditious intention”) provides very little comfort for members of the communities who are likely to be targeted by the authorities. Just as with the detention and control order provisions, the crime of sedition can be used by the authorities to persecute and harass members of the communities they regard as posing a threat to Australia’s national security. This will have the effect of further dividing the Australian community into those who are regarded as posing no actual or potential threat of terrorism and those who are suspected of posing such a threat in a general climate of suspicion and threat creating resentment and hostility among targeted groups and individuals. This runs the distinct risk of converting resentment and hostility into violent and terroristic intent, a sort of self-fulfilling prophecy providing the government and national security authorities with a ready-made defence against charges that they are unfairly targeting certain groups and individuals. A more deeply and dangerously divided Australian community will be the result. Thus, the community legal sector will have to be vigilant and energetic in defending the national security of the country from the national security authorities whose efforts to protect national security may in fact only serve to undermine it.

5 Conclusion

The Australian Government's recent national security and anti-terrorism legislation presents considerable challenges for the community legal sector. The series of bills enacted since September 11 2001, the culmination of which is the Anti-Terrorism Bill (No. 2) 2005, removes many of the freedoms and rights that Australians have for many years been able to take for granted. In particular, the detention and control orders degrade the importance of the role of formal trials and the production of credible evidence by the prosecution in the administration of justice in this country. The newly-defined crime of sedition provides the Australian Government and national security authorities with the ability to further centralise power in their hands under the pretext of protecting Australia's national security. Suspect groups are likely to be the targets of these provisions leading to resentment and hostility among them, emotions and attitudes that can easily be inflamed into a lust for revenge and violence by community leaders with the will and the means to do so. The community legal sector, despite its meagre resources, will be required to play a crucial role in informing and educating the Australian people about the implications of the legislation for their freedoms and rights. Just as with the legislation itself, the sector will have to 'target' its CLE activities on suspect groups and individuals without compromising its ability to provide basic legal services to other poor and disadvantaged Australians. This is the routine, unglamorous role it is funded to perform by the Government. The sector will thus have to avoid being drawn into self-destructive conflict with the Australian Government. This could be a very tall order indeed.

References

Attorney-General's Department (AGD) (2005) Commonwealth Community Legal Services Program Guidelines (August). Available at http://www.ag.gov.au/agd/WWW/cclsphome.nsf/Page/Guidelines. (Accessed 23 January 2006)

Australian Government (n.d.) 'Australian Laws to Combat Terrorism'. Available at http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/826190776D

49EA90CA256FAB001BA5EA?OpenDocument. (Accessed 27 April 2006)

Emerton, P (2004) 'Paving the Way for Conviction without Evidence—A Disturbing Trend in Australia's "Anti-Terrorism" Laws', *Queensland University of Technology Law and Justice Journal*, vol. 4, no. 2, pp. 129-166

Federation of Community Legal Centres (Vic) Inc. (2003) Submission to the Senate Legal and Constitutional Committee Inquiry into Legal Aid and Access to Justice, September

Head, M (2005) 'Orwell's Nineteen Eighty-Four 20 Years On: "The war on terrorism", "doublethink" and "Big Brother"', *Alternative Law Journal*, 30: 5 (Oct), pp. 208-213

Hocking, J (2005) 'The Anti-Terrorism Bill (No. 2) 2005: When scrutiny, secrecy and security collide', *Democratic Audit of Australia*, November: 1-4. Available at http://democratic.audit.anu.edu.au/ (Accessed 23 January 2006)

Howie, L (2005) 'The threat of terrorism and social change', *Human Rights Defender* Special Issue: The Anti-Terrorism Bill (No. 2) 2005. November/December: 22-23

Jackson, H (2005) 'The power to proscribe terrorist organisations under the Commonwealth Criminal Code: Is it open to abuse?', *Public Law Review*, 16: 134-151

McDonald, M 'Be Alarmed? Australia's Anti-terrorism Kit and the Politics of Security', *Global Change, Peace and Security*, vol. 17, no. 2 (June), pp. 171-189

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

NACLC (2003) *Doing Justice: Acting together to make a difference*, Sydney South, NSW

NACLC (2003a) Submission to the Senate Legal and Constitutional Committee Inquiry into Legal Aid and Access to Justice, September. Sydney South, NSW

Nettheim, G (2005) 'Terror Australis: the "debate" to date', *Human Rights*

Defender Special Issue: The Anti-Terrorism Bill (No. 2) 2005. November/December: 6-8

North, J (2005) Interviewed by Tanya Nolan on the AM Program, Thursday, 1 December 2005. Available at http://www.abc.net.au/am/content/2005/s1520535.htm (Accessed 20 January 2005)

Rix, M (2005) 'Divided Loyalties? The New Public Management of Community Legal Centres', *Third Sector Review*, vol. 11, no. 1, pp. 51-66

Ruddock, P (2005) 'Government Enhances Anti-Terror Bill'. Media Release 222/2005. 1 December 2005. Available at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases (Accessed 20 January 2006)

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 (Accessed 20 January 2006)

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.

11

E-courts: toward information protection management structures

Lauren May and Mark Burdon

Information Security Institute, Queensland University of Technology

Abstract

This background paper is concerned with ensuring the integrity of Australia's e-court processes through the development of information protection standards and protocols. The integrity of the court process is important to the national interest because businesses and citizens depend on the certainty of court decisions, naturally assuming that their information and privacy is protected. This paper is a catalyst for future research leading to the creation of an information protection framework, including policies and standards enabling courts to define the use of courtroom technologies, thus ensuring that their design and application is grounded within established information protection principles. Without substantiation of the quality of technological structures and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain.

Keywords: e-courts, courtroom technology, security framework, security management, information standards

1 Introduction

Contemporary information technologies (IT) constitute infrastructures upon which our societies now rely. Our court system is no exception even though the introduction of new technology into the mainstream has been at a slower, more cautious rate than other governmental and industrial sectors. Interactions with courts are still predominantly paper-driven but the development of electronic courts (e-courts) and concomitant electronic processes are experiencing a shift from traditional silo-based working structures to new business processes and systems. Initially, IT was solely used as an automation and presentation tool. Today's information communication technologies (ICT), however, allow for systems which are more sophisticated and modularised with potential for broader and deeper capacity.

This paper contends that a comprehensive information security perspective is required to augment wider environmental structural implementation, thus ensuring the secure protection of sensitive

information at the infrastructure level. Accordingly, formalised industry standards and best-practice guidelines should be developed regarding the use of e-courts and electronic court processes.

1.1 Information protection defined

The research project is cross-disciplinary by nature to enable the researchers to undertake a comprehensive and rigorous assessment of the legal and technological implications of information security practices in the court domain. The disciplines of law and information security bring with them their own languages and cultures. A starting point in the research has been to establish an agreed vocabulary of terms for words that have different meanings to both disciplines. For example, when a technologist talks of 'integrity' they mean definitively that a certain piece of information has not been changed whether accidentally or on purpose. A legal professional or law academic, however, refers in the abstract to notions of ethical behaviour.

Accordingly, an aim to resolve in law and information security cross-disciplinary research is learning, accepting and defining a common and agreeable language to frame research questions.

Language issues are readily visible when court practitioners (solicitors, barristers and judges) are asked about "information security". Preliminary discussions have revealed that the term appears to carry technological and/or negative connotations with which court practitioners do not associate as being within their realm of interest. This reflects the hierarchical nature that pervades legal cultures which clearly delineates between senior/junior staff and practitioner/support personnel. Hence "information security" appears to have an isolating effect indicating that it is viewed by court practitioners as a solely technological issue to be resolved by IT support staff.

Alternatively, "information protection" appears much more acceptable to court practitioners possibly because it is an all-inclusive term that reinforces their cultural notions of ethics and confidentiality, with which they do associate. Experience indicates that successful information security applications include an environment of staff participation. As a consequence, in the context of this paper and the ongoing research, "information protection" is synonymous with "information security".

2 E-courts and courtroom technologies defined

Different definitions of an e-court currently exist. Commonly, an e-court refers to the concept of a court that has the facilities to operate a “paperless trial” (Nicholson, 2002, 66), (Potter, 2004, 2), (Lederer, 1999, 800). The definition envisages a physical court which uses courtroom technologies during trial and pre-trial proceedings. Courtroom technology is in itself a generic expression used to describe numerous forms of technology that may or may not be collectively present in any given courtroom (Lederer, 2005, 676). Courtroom technologies typically include document imaging systems, real time transcription software, case management databases, video conferencing facilities, digital video and audio recording, access to the Internet, e-mail and external intranet access.

Alternatively, the Federal Court of Australia defines an e-court as “a web-based forum which the Federal Court uses as a virtual courtroom for giving directions and other interlocutory orders on-line. When using eCourt, the Court may receive submissions and affidavit evidence and make orders as if the parties were in a normal courtroom.” (Practice Note No. 17, 2001). The Federal Court’s e-court is not a physical courtroom and has limited functions as it facilitates a process for handling interlocutory matters only and does not cover all aspects of trial proceedings (though it is acknowledged that the Federal Court does foresee using an actual courtroom for certain trials involving courtroom technologies).

The Productivity Commission, in their review of government services adopt a different definition for “electronic courts” (Productivity Commission, 2005, 6.6). This definition refers to court systems, such as the PERIN Court in Victoria which is designed to “resolve large numbers of unpaid infringement notices in such a way as to reduce the load on the judicial and administrative resources of the hearing courts”. This definition of “electronic court” refers to a fully automated IT process that automatically imposes fines on unpaid infringement notices and does not involve any trial proceedings and does not refer to an actual physical court environment.

The researchers recognize the flexible terminology regarding e-courts. For the purposes of this research, an e-court is defined as a body with an

adjudicative function that makes use of ICTs to run its proceedings. The definition refers to an actual, physical courtroom. It is broad in scale to encompass different types of courts and to include aspects of both the "paperless" and "virtual" courtrooms mentioned above. The research does not cover fully automated "electronic courts" or commissions of inquiry. The ICTs referred to are the courtroom technologies detailed above, though it should be noted that the technologies mentioned are not intended to be an exhaustive list.

2.1 E-courts and courtroom technologies in Australia

Australia has been one of the frontrunners in the development of e-courts and courtroom technologies (Lederer, 2004, 640) (Wallace, 1999). Initial development was reactive in nature, in the sense that new courtroom technologies were implemented to meet fresh demands caused by the specific requirements of several very complex pieces of criminal and civil litigation, and also by lengthy commissions of inquiry in the early 1990s (Macdonald and Wallace, 2004, 649). For example, the Estate Mortgages litigation in Victoria involved twelve active parties, who instructed a total of 27 counsel, which led to an estimated cost of $500 per minute to run proceedings (Smith, 2001). The Wood Royal Commission into police corruption in NSW took two and a half years to conclude.

Given the large cost and the length of time complex commissions of inquiry and litigation can take, it is not surprising that courtroom technologies were implemented to increase the efficiency and the effectiveness of court proceedings. Implementation has proceeded to the extent that courtroom technologies are now standard in royal commissions (Macdonald and Wallace, 2004, 650). Commonwealth, State and Territory courts all rely on ICT to varying degrees during their proceedings, though some jurisdictions are more advanced than others. That said, e-courts are still only used during matters of complicated and large-scale litigation, such as the Channel 7 v Foxtel case currently being heard in the Federal Court.

2.2 Integrated e-court structures

The first phase of technological development within e-courts was the

application of the courtroom technologies themselves. In a sense, the initial impetus was on building more sophisticated automation and presentation tools. The succeeding years saw a shift in focus from the tools themselves to the technological structures that support those tools. The Federal Court of Australia's e-court Integration Project (Sherman and Stanfield, 2004) encapsulates thinking on e-court process realignment and State examples of developing technological structures can be seen in Victoria (Victorian Law Reform Commission, 1999) (Warren, 2005) and Queensland (Sherman and Sims, 2002).

Court systems are moving to a position that other government sectors and industries reached during the last decade, namely, implementing ICT to improve efficiency and effectiveness by replacing traditional manual, paper-based systems. Courts have been relatively late adopters of ICT and it is hoped that further research will provide a clearer indication of why that has been the case. The researchers' preliminary hypotheses suggest that cultural issues within the legal profession may have been a factor. The practice of Common Law justice is conservative as it is dependent upon evolutionary principles through the application of centuries' old legal precedent. The implementation of ICT is a revolutionary process as the act of technological integration slices through many traditional working structures and practices. Moreover, there are multiple senior executives within court systems (judges, court administrators, senior barristers) and the impetus for change may well be fractured and disparate. Therefore, the driver for ICT implementation may not exist at a senior level and may even take the form of a conscious or sub-conscious resistance to change. It should not be underestimated how attached senior judges and lawyers are to the paper-based world.

3 Information protection issues

As ICT usage comes of age, these structures and technologies become part of the wider information infrastructures which define modern societies– our critical information infrastructures. Critical infrastructures are defined by the Australian Government as those facilities which, if compromised for an extended period, would significantly impact upon the well-being of the nation. Critical infrastructure protection is concerned

with ensuring the integrity of the nation's critical infrastructures. This is achieved through a number of approaches, one of which is ensuring the integrity of the court process which directly affects integrity of law enforcement and crime prevention (TISN, 2005).

The integrity of the court process is akin to a critical infrastructure and it is important to the national interest because litigants depend on the certainty of court decisions. An intrinsic reliance is placed on courts and law firms to protect their clients' information and privacy during the litigation process. This reliance has perhaps not been fully translated to e-courts. A potentially disturbing trend within court practitioners is the inherent assumption or reliance on third party providers that courtroom technologies are somehow automatically 100% "secure". "Other industry" experience shows that industry-level security services are most successfully achieved through a holistic approach - through the creation of an information protection framework, including policies and standards, designed specifically for the required environment.

3.1 Literature review on information protection in e-courts

Although the more generic information security discipline is well-represented in public domain literature, the literature review research revealed only one paper with specific reference to information protection issues in Australian e-courts. This paper raised fundamental issues with respect to the relationship between actual technological security mechanisms and their perceived deliverance of security services to the court environment (Caelli, 2003). Another relevant paper that should be noted is that of The Law Society of New South Wales which published an issues paper looking at information security concerns regarding online transactions with particular attention on authentication (Kay, 2001). The Law Society paper is limited in focus to the extent that it only covered the processes involved in electronic filing of documents from predominantly a practitioner's point of view whereas Caelli's paper provided a critical approach to structural e-court information protection questions.

A minimal number of international references were also retrieved. Most references were American and this is not entirely surprising given that e-courts are more established in the USA than Australia. In general, individual court practitioners within their respective legal professions

raised issues indicating that the professions are still wrestling with the development of new ICTs.

3.2 An information protection experience in the USA

The National Center for State Courts (NCSC) is an organisation whose mission is to “improve the administration of justice through leadership and service to state courts, and courts around the world”. At the 2004 NCSC e-court conference, participating court practitioners raised a number of information protection issues.

Messing and Teppler (2004) discussed transparency and reliability challenges facing e-court processes with an emphasis on “preventing a pandemic of judicial identity theft”. They provided a real-life example of how court employees in Richmond, California illegally altered criminal records to show that charges had been dismissed against five defendants when in fact they had not. The employees accessed court records by remotely dialling into the court’s case management database using passwords obtained whilst acting as consultants to the local police force. The authors concluded that “no longer can we presume courts have authoritative record of electronic filings unless court computer security is technically assured” (Messing and Teppler, 2004, 12).

Messing and Teppler also discussed trust issues arising where the integrity of judicial orders, for example, may come into question. “Integrity” in this context refers to the property that the judicial orders have not, either accidentally or on purpose, been altered during communication and storage after the order has been made. The contribution of this paper is in raising awareness that information protection is needed for e-court applications. Other presentations at the same conference pointed out quite realistic scenarios of information system “glitches” that have the potential to undermine the authority of the judicial process. Each also pointed out that all these issues could be overcome with information security approaches which have been tried and tested in other industry information infrastructures.

Many of the potential consequences highlighted by the NCSC e-courts conference are pertinent to Australian courts within a “lessons learned” technology application perspective and a cultural acceptance viewpoint.

3.3 Implications for Australian e-courts

In his 2003 address to the “Courts for the 21st Century: Public Access, Privacy and Security” conference at the QUT School of Law, Caelli addressed some prospective pitfalls by highlighting inherent technological security issues with respect to a recently published e-court proposal in the Sydney Morning Herald newspaper. The presentation focused on several fundamental information protection mechanisms and widely-accepted design misconceptions including connectivity, end-to-end secure channels, archiving, time/date stamping and signing of documentation (Caelli, 2003).

The degree of instability and potential insecurity has thus far been small because the adoption of court technologies has been relatively limited. Our preliminary findings indicate that court systems are moving to expand the use of courtroom technologies and to re-align existing processes around ICTs. Consequently, the scope of the potential problem will increase commensurate with the implementation of these new technological structures and processes that have not been conclusively tested within an information security context.

Messing and Teppler (2004) provided a realistic and foreseeable example of problems when they highlighted the possibility of accidental or deliberate alteration of judicial decisions with no recourse to audit trails or management systems to validate integrity. It is these issues of trust that could cause significant damage to the reputation of the court and the judicial process because our society places so much confidence in the belief that our personal information will be kept secure when we interact with the courts and the legal profession. At the same time, our society consents to follow the rulings of the court whether they are thought to be right or wrong. The whole system is based on trust and confidence. For this reason alone, it is vital that courts have total confidence in the integrity of their new technological systems for society to maintain its trust in court decisions.

4 Next steps: information protection and ICT in e-courts

The focus of our research is to develop information protection management structures to ensure maximum worth of ICT usage and to

maintain the confidence that society demands of our court systems. This involves identifying usage properties and matching these with well-understood techniques leading to the creation of an information protection framework to certify that e-court applications are grounded within firm information security principles.

The usual path to ICT acceptance within any given industry is: first, a period of individual trial-and-error ad hoc approaches, generally aimed at replacing manual processes; second, realisation of the need for interoperability, away from numerous information “silos” towards a more manageable system; third, recognition of the requirement for standardisation, in line with alternative good business practices; and, finally, acceptance of the formalisation of the management of information into the normal business management structure. As a general rule, the more advanced is the industry along this path, the more mature is the contribution of the technology to the industry and the more accepting is society towards that industry’s credibility and authority.

In an ICT-driven world, court practitioners are faced with the same issues as any other industry. American court systems are currently at the second stage and fast approaching the third: the recognition that interoperability and standardisation are paramount. For example, the Sedona Conference is a research and educational institute dedicated to the advanced study of law and policy including complex litigation (Sedona Conference, 2006). The organisation has developed a series of best practice guidelines for managing electronic records that would be directly relevant to Australian e-courts (Sedona Conference Working Party, 2005). The American Bar Association’s Information Security Committee (ABA ISC) also explores legal and technical aspects of information security from the perspective of the legal profession. Again, their work could be relevant to Australian legal professions (ABA ISC, 2006). Accordingly, it is an aim of this research to extrapolate lessons learnt from the USA and apply these experiences to the Australian situation.

4.1 An information protection “set of standards” for e-courts

Information protection standards provide for the quality service of technology by applying protection techniques and mechanisms to achieve fundamental security goals and services. Typically information

security goals include services such as confidentiality of data, integrity of information, authentication of data source, non-repudiation and availability of data. Protection mechanisms are the managerial and technological methods, protocols and primitives which are employed in order to achieve the desired information goals. Standardisation is therefore about taking a holistic approach to the business functions being fulfilled. An essential foundation for this approach is that of information protection whose main goal is to ensure the quality of information.

The research project aims to develop a conceptual “set of standards” that are linked together in a hierarchical (or triangular) structure, as detailed in Figure 1.

Figure 1. Set of Standards Triangular Concept

Relevant issues are addressed from a high conceptual design and upper management level (at the peak or vertex of the hierarchy), through the medium application management and implementation level and onto the lower best-practice guideline checklist operational level (at the broader baseline of the hierarchy).

Further formal research and development leading to the final stage of IT acceptance highlighted above- formalisation of the management of information into the normal business management structure- is therefore the ultimate goal of the research project. The team of researchers from QUT includes law and information security academics as well as industry partner organisations. The team’s intention is to develop this project through the Australian Research Council (ARC) system.

The research team will concentrate on specific topics considered pivotal to the essence of the project. These include initially investigating the nature of court documents and understanding the concepts of risk and trust in the context of court environments. Surveys, interviews and case studies will ensue to determine the current Australian e-court experience. Guidelines will be developed including costing and best-practice modelling, concluding with recommendations towards a governance standard for e-courts including a protection profile under Common Criteria. Tangible outcomes of the research project will be the creation of an information

protection framework that satisfies both long-established information protection principles and newly emerging standards at both the national and international levels.

5 Conclusion

The wisdom of ICT usage within contemporary court and legal environments is still a matter of debate because legal processes are still largely paper-based. This research paper has established that, regardless of philosophical attitudes, ICT usage is occurring today within the court and legal environment and is showing signs of increasing. Without substantiation of the quality of technological structures and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. Any degree of instability could weaken trust and confidence in the court system at a local, national and international level. This in turn could have direct consequences on national security because the maintenance of law and order is partly dependent upon the degree of certainty our society demands from the courts.

There is a need for standardisation of ICT applications in the e-courts environment based upon an information protection foundation to maintain confidence in new technological court processes. There is a scarcity of literature and formal research in the public domain addressing this issue and further study is required. We conclude that formalised industry standards and best-practice guidelines should be developed to ensure the integrity of Australia's e-court processes.

References

American Bar Association. 2006. *Section of Science & Technology: Information Security.* http://www.abanet.org/dch/committee.cfm?com=ST230002 (accessed 19 April 2006)

Caelli, W. 2003. E-Security, Information management and archiving in the public sector. In *Courts for the 21st Century: Public Access, Privacy and Security Conference, 6 November, 2003, Queensland University*

of Technology, Brisbane, Australia. Queensland University of Technology. http://www. law.qut.edu.au/files/ecourts-qut-061103.pdf (accessed 12 October 2005).

Federal Court. 2001. *Practice Note No 17 - Guidelines for the use of information technology in litigation in any civil matter.* http://www.law.mq.edu.au/Units/law404/E-Court%20FCA%20Practice%20Note. htm. (accessed 26 September 2005).

Kay, S. (2001) Security and authentication requirements in the court process : part 1 : current security practices and requirements and survey of courts' approaches to online security in Australia and the US., *Internet Law Bulletin*, Vol. **4**, pp. 5-13.

Lederer, F. I. (2005) Technology-Augmented Courtrooms: Progress Amid a Few Complications, or the Problemtic Interrelationship Between Court and Counsel, *New York University Annual Survey of American Law*, Vol. **60**, pp. 675-709.

Lederer, F. I. (2004) What have we wrought?, *William and Mary Bill of Rights Journal*, Vol. **12**, pp. 637-48

Lederer, F. I. (1999) The road to the virtual courtroom? A consideration of today's--and tomorrow's--high-technology courtrooms, *South Carolina Law Review*, Vol. **50**, pp. 799-844.

Macdonald, R. and Wallace, A. (2004) Review of the extent of courtroom technology in Australia, *William and Mary Bill of Rights Journal*, Vol. **12**, pp. 649-59.

Messing, J. and Teppler, S. 2004. Preventing a pandemic of judicial identity theft: Transparency and reliability challenges facing ecourt processes and output today. In *2nd NCSC E-Courts Conference, 13 December, 2004, Las Vegas, United States of America.* National Center for State Courts. http://www. e-courts.org/presentations/messing.pdf (accessed 10 October 2005)

National Center for State Courts. 2006. *NCSC Mission Statement.* http://www.ncsconline.org/ (accessed 17 January 2006).

National Center for State Courts. 2005. *2nd E-courts Conference.* http://www.e-courts.org/ (accessed 10 October 2005).

Department of Justice, Victoria. 2006. *PERIN Courts*. http://www.justice.vic.gov.au/CA2569020010922A/ page/Courts+and+Tribunals-Perin+Court?OpenDocument&1=0-Cou

rts+and+Tribunals~&2=0-Perin +Court~&3=~ (accessed 19 April 2006)

Productivity Commission 2005, *Report on Government Service,* Productivity Commission, Canberra. http:// www.pc.gov.au/gsp/reports/rogs/2005/chapter06.pdf (accessed 13 October 2005)

Sedona Conference. 2006. *The Sedona Conferences.* http://www.thesedonaconference.org/ (accessed 19 April 2006)

Sedona Conference Working Party 2005, *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age,* Sedona Conference. http://www. thesedonaconference.org/content/miscFiles/TSG9_05.pdf (accessed 19 April 2006)

Sherman, J. and Sims, I. 2002, *Supreme & District Courts: IT Action Plan – 2002,* Queensland Courts, Brisbane. http://www.courts.qld.gov.au/publications/SJA/IT%20Action%20Plan _small.pdf (accessed 13 October 2005).

Sherman, J. and Stanfield, A. 2004, *Federal Court of Australia: eCourt Integration Project - Final Report,* e.Law Australia Pty Ltd. http://www.aph.gov.au/senate/committee/legcon_ctte/estimates/bud _0405/ ags/155_att.pdf (accessed 12 October 2005).

Smith, T. 1998. *AIJA Annual Conference - The Estate Mortgage Court System*. http://www.aija.org.au/ conference98/notes/sess1.html (accessed 19 April 2006)

TISN.2005. *About Critical Infrastructure Protection* http://www.cript.gov.au/agd/www/TISNhome.nsf (accessed 19 April 2006)

Victorian Law Reform Commission 1999, *Technology and the Law,* Government Printer, Melbourne. http://www.egov.vic.gov.au/pdfs/techlaw.pdf (accessed 4 October 2005).

Wallace, A. (1999) The challenge of information technology in Australian courts. *Journal of Judicial Administration*, Vol. **9**, pp. 8-36.

Warren, M. (2005) Modernising justice: IT and the Supreme Court, *Law Institute Journal*, Vol. **79**, pp. 44-5.

12

Citizen participation platform guaranteeing freedom of speech

Emilia Pérez, Ana Gómez, Sergio Sánchez, Jose D. Carracedo, Justo Carracedo, Carlos González, Jesús Moreno

Departamento de Ingeniería y Arquitecturas Telemáticas de la Universidad Politécnica de Madrid & Observatorio para la Democracia Digital y los Derechos de la Ciudadanía en Internet

Abstract

This paper presents a proposal for an advanced system of debate in an environment of digital democracy from a multidisciplinary perspective (specifically, sociology and telematics). Unlike previous works, it includes new functionalities required to ensure the authentication of participants while allowing for the anonymous participation of users that desire it, where the system is unable to disclose or even to know the identity of system users. Furthermore, this proposal allows for verifying the proper function of the system, free of tampering or fraud intended to alter the conclusions or outcomes of participation.

Keywords: e-democracy, e-government, freedom of speech, anonymity, telematic platform

1 Introduction

Far removed from day-to-day politics, the advent of telematic systems of citizen participation and management has been presented in the abstract as a solution to the present-day crisis of legitimacy, trust and participation broadly affecting institutional democracies (both representative and parliamentary). Teledemocracy, cyberdemocracy, e-administration, e-democracy, e-government, electronic government, digital government, electronic government, electronic democracy, digital democracy are a series of terms that appear ever more frequently in the popular media; they feature in electoral programs, in public statements by politicians and in general plans aiming to further the development of the "information society." Nevertheless, there are significant differences between the meanings given to these terms. This lack of definition directly affects plans for developing the information society, as an initiative can easily bill itself as "an advance towards digital democracy," in the absence of standard parameters for validating it as one. Such projects in public affairs carry an additional risk, for no standards exist for evaluating the results of initiatives undertaken, as they are often proposed, designed and executed by researchers of an exclusively technical background.

The lack of theoretical clarity allows telematic or electronic voting to be presented as experiments in digital democracy; while this is a common tool in democratic systems, it is by no means the only one. It is also true that present democratic systems privilege voting at the expense of processes of information and discussion. It is also believed that computer-mediated communications enables the pursuit of solutions independently of objections, which have made systems of direct democracy unfeasible for over two hundred years (due to scales of territories, sizes of populations and lack of qualified knowledge to responsibly make decisions).

Thus, the problem around digital democracy lies in the fact that it reopens the debate on forms of democratic organizations. This is important to study because it must allow for identifying the functions and characteristics to be developed. The properties and potential of information and communication technologies (ICT) gives rise to imaginative speculation regarding a multitude of models consistent with

the political conceptions of each community (Gilbert 2003). We have observed, with particular doubts, how present implementations of ICT often expand the possibilities of social control– even in platforms of telematic participation- and generally deepen the construction of what David Lyon (2001) calls the *surveillance society*. It is obvious that in most democracies there is no exercise of (citizen) democratic control over processes of technological innovation or analysis of its consequences. Faced with this reality, our research group considers itself intellectually committed to a line of investigation that seeks to deepen, develop and implement computer systems that enhance citizen rights and minimize the possible negative effects on these rights by the establishment of the *network society*.

In our view, the plethora of possibilities offered by digital democracy would tend to strengthen processes rooted in classical conceptions of direct democracy. Our VOTESCRIPT group is committed to the development of telematic systems that would enable free public participation with the aim of promoting both the mutual relationships of citizens to each other and citizens' relationships with authorities in a way that allows them to draw conclusions that facilitate decision-making, based on their own discussions. The method of applying the results of these discussions and whether they are to be binding or not, are issues that are beyond the scope of this group, as those issues fall within the domain of public affairs.

2 Conceptual framework

Our analysis of the experiential studies (DEMOS 2003; DUNES 2005; EURO-CITI 2002; Luehrs, Pavón & Schneider 2003; WEBOCRACY 2004), both in Spain and in the rest of Europe, as well as our sociological fieldwork, have allowed us to draw a series of conclusions on the characteristics that must be part of any system of citizen participation in order to achieve public acceptance:

1. First, the problem of digital stratification must be confronted. Though there are fresh government initiatives daily backing the introduction of computers across demographics, there still exists a high percentage of the population which is information technology

(IT) illiterate. Particularly for these people, it is essential that citizen participation systems are simple and easy to use.

2. The issues under discussion must be close to the participants' concerns. On this point, participation systems orientated to local issues have proved very attractive for local communities.
3. There must be a commitment by the relevant authorities that the conclusions arising from a debate are taken into account in a final decision. It has been found that one of the most negative aspects affecting the success of a given forum is that opinions offered hold merely testimonial value, or that mechanisms have not been clearly defined to transmit these opinions to the pertinent bodies. The promises and expectations generated by the process must be respected and fulfilled if citizen participation is intended to grow.
4. The discussion process must be clearly structured into well-defined phases: selection of subjects of interest, expression of participants' opinions and the drawing of conclusions. The last phase can be undertaken through an automatic or semi-automatic procedure that extracts knowledge from the messages emitted, which can be followed by dynamics of conciliating postures and consensus building or even voting processes.
5. The system must guarantee certain aspects relating to the identity of participants, or their anonymity, if desired, secure storage of information and its freedom from tampering.

2.1 The issue of security

The issue of security would appear to suffer from the most neglect in systems of digital democracy. It has been seen that most of the open forums in municipalities do not perform any type of access control over the participants, or this control is incomplete, in such a way that systems can be flooded with messages from participants who are not entitled to respond on the matter under discussion. Often, this lack of security results in messages that are insulting, or in breach of protocols of participation, or even in conscious practices of sabotage of the discussion process. In contrast to this model, and to avert chaos, we have found other systems in which participants are clearly identified but also subject to possible monitoring. This also constitutes an impediment to free

participation, as participants may feel that their involvement is under surveillance, and such sentiment may have serious consequences, particularly in smaller communities. In our sociological work, one of the main concerns regarding cyberspace is the lack of anonymity, the sensation of lack of privacy in daily activities. In systems of participation, to ensure freedom of speech, we believe it is crucial for participants to have mechanisms that can ensure their anonymity in certain conversations.

Bearing in mind these security considerations, a series of good operating principles have been identified that should be guaranteed by any platform of digital democracy, independently of the honesty and professional abilities of the persons responsible for operating the system:

- Freedom of speech, whereby all users of the platform can express themselves with no fear of reprisals in the present or in the future.
- Equality, whereby the opinions of all citizens carry the same importance.
- Mutual respect. Opinions expressed publicly must observe certain rules that have been defined and accepted by the participants in the forum themselves.
- Determinate duration of discussions. Subjects for discussion shall have a lifetime that is agreed and known by users when the debate commences.
- Auditable. Citizens should have robust probes in order to verify that the system is functioning properly.
- Validation of conclusions either by consensus or through a vote. In the latter case, the system must ensure a clean voting process.

2.2 PARTICIPA system

The authors of this paper have designed a system (PARTICIPA) which overcomes the limitations of existing systems. As a result, we have obtained a telematic and protocol communication architecture which easily adjusts to the needs of different human groups and which may be configured and extended according to management needs.

We have been especially careful in applying security procedures in telematic systems, for they are to offer citizens the guarantees that society demands. New functional tools have been included to ensure user authentication and to permit anonymous participation while preventing

participation by non-entitled persons who do not belong to the authorized group from giving their opinion. Citizens are provided with tools that will allow them to verify proper system operation against tampering or fraud intended to modify the conclusions or the results of the participation. All these tools guarantee important aspects of both a social and technical nature, most importantly: freedom of expression, equality and auditibility. This work is part of the research activities being performed by this group in the project “Development of a secure telematic platform bearing digital democracy scenarios” (Project TIC 2003-2141), under subsidy of the Spanish Ministry of Industry, Tourism and Commerce. The project aims to develop a platform for digital democracy that would include the security services discussed herein (Gómez et al. 2005b).

3 Global architecture of PARTICIPA system

To meet the demands of society, the system must be equipped with robust security systems. The proposal herein involves the use of cryptographic algorithms with symmetrical and asymmetrical keys, opaque and blind signatures in the use of smart cards (Carracedo 2004).

Below are definitions of the entities of this platform, followed by an outline description of the global performance of the debate system. A detailed description of the information flow between them is beyond the scope of this article, though it is fully explored in (Gómez et al. 2005c).

3.1 Participating entities

The platform proposed herein involves a series of automatic systems that operate with software based on code that has been previously published, thus providing for the possibility of auditing by the relevant entities. Figure 1 depicts the relationship between the following systems:

- Participation Points. Users will interact with the system through computers that are connected to the Internet and equipped with smart card readers.
- Registry. This entity will authenticate users and return them the authorization that will enable them, at a given time, to obtain an alias for their anonymous participation or cast a vote.
- Registry Intervention Systems. Complementing and supervising the

task of the Registry, these perform the same processes in a parallel fashion.

- Forum. This entity supports the debates that take place in the system, receiving and publishing opinions of authorized users and storing all communication transactions received in order to enable functional audits if required.
- Alias Manager. This entity ensures that there are no repeated aliases in the system.
- Conclusions Extractor. Knowledge is extracted through a semantic analysis of the information published in the forum during a discussion. Mainly, it will extract the main lines of argument in order, ultimately, to submit them to a vote.

Figure 1. System agents

3.1.1 Voting system

The voting system manages the voting process in the phase of conclusion validation. In addition to the above entities, the following persons participate in the system:

- Users. Each person registered in the census of participants can interact with the system as a user, either through observing discussions or through issuance of opinions in the forum. All users can participate in the vote on conclusions after the debate.
- A registry manager, responsible for the maintenance of the Registry system.
- Registry monitors responsible for each of the Registry Intervention Systems.
- Moderator. Responsible for ensuring that debates stay on the subject for which they were created.
- Guests. Users that may participate, in a fully identified manner, in the different phases of the discussion process even though they are not in the census of participants.

3.2 Forms of participation

The system envisages two forms of participation in issuing their opinions in a forum or discussion. First, anonymous participation through use of an alias. Second, identified participation, that is, with use of one's real identity with a name and surname. Participation in voting is anonymous in all cases.

3.3 Overall function

Each debate forum has a census of individuals that are allowed to participate. It is beyond the scope of this article to determine which citizens are entitled to participate in a given forum; rather, we begin from the premise that some legitimate authority has created the proper census.

Authorized citizens shall therefore have a Participation Card, which shall consist of a tamper-proof smart card that will serve to identify users and to support critical cryptographic processes. This will prevent fingerprints from previously used computers from being incorporated into subsequent attacks. Moreover, this card would store receipts of the operations performed, which would be useful in case of detection or suspicion of system malfunction.

When a citizen wishes to give an opinion in a forum for which he or she is authorized, they must report with their Participation Card to one of the Participation Points, where they can provide their opinions and participate in voting.

If a user wishes to participate in a forum anonymously, the user must first complete a dialogue with the Registry entity to obtain authorization that would allow the user to negotiate an alias with the Alias Manager. This username is obtained with the blind signature mechanism and will have a pair of public/private keys that will allow the user to sign messages sent to the forum without being identified, thereby ensuring that the messages have come from an authorized user.

The process of obtaining an alias offers the apparently contradictory guarantees of authenticity– only authorized members can participate in the debate– and of privacy, for the system ensures users' anonymity, so that the system itself cannot link the alias to the user. Furthermore, the system prevents use of the same alias by more than one participant in the forum.

The operations of the Registry are supervised and monitored in parallel fashion by the Registry Intervention Systems, so that the Registry is deterred from any temptation to issue more than one alias authorization to a single member, the issuance of authorizations to false members or in the name of those who have not requested it, or arbitrary denial of said authorization. In order to ensure that opinions have not been altered, messages generated are signed in either anonymous or identified status, as relevant.

After verifying the source of the message, the Forum signs and returns a receipt that is stored in the Participating Card. The purpose of the receipt is to dissuade system managers of the temptation to modify messages or to feign non-reception. After confirming that the content accords with the publication policy, the Forum publishes the message or stores it in a protected place, wherein it notifies the author of the reasons for which the message has not been published.

After the deadline for emitting opinions has passed, the Conclusion Extractor generates the main lines of argument on the basis of the messages received. In addition, the proposed system envisages the possibility of submitting conclusions to a vote. The complexity of the voting system can be modulated in accordance with the interests at stake.

3.4 Extracting conclusions and voting on the results

Once the discussion forum is closed, the conclusion phase begins, in which the Conclusion Extractor generates, through a semantic analysis of the message published by users, the diverse conclusions or lines of argument followed in the debate.

For the purpose of validating the conclusions extracted and determining the most suitable one, they are submitted to vote. The process affords the guarantees of security and anonymity required for a system of telematic voting (Gómez et al. 2005a) and all system users registered in the census may participate.

The security requirements demanded of this type of system will depend on the interests to be protected in each voting process. In cases where users believe that the importance of the subject should require strong security, use of a complete system of telematic voting, which meets all the security requirements of telematic voting at the highest level, is suggested.

Nevertheless, it is reasonable to assume that subjects with lesser interests at stake and where the benefits of possible fraud are lower, a reduced version of the system might be advisable.

After the voting process and achievement of results, these are transferred to the Forum, which makes them public.

4 Conclusions

Systems of digital democracy are still in a period of maturation, both from the technological point of view and from a functional, social one. In this first phase, digital democracy must be brought to the citizens through the design of attractive systems that are easy to use and which arouse their interest. Moreover, public authorities must lose their suspicion of systems of digital democracy– for these constitute the most direct form of control by citizens over decisions affecting them- and instead lend full support to their use in decision-making processes.

After this stage of *making contact* is overcome, systems of citizen participation must increase the services they offer in order to be useful in more critical environments, realms in which there may be a manifest interest on the part of individuals, organizations or authorities to not adequately reflect the participants' opinions, with the aim of reaching certain conclusions. For these circumstances, the system of citizen participation should contain mechanisms for detecting any possible anomalies in the system, such as the loss or alteration of messages.

Moreover, there are numerous scenarios of citizen participation in which users consider possible anonymous participation to be a requisite for participation. In these cases, anonymity must be provided with the due guarantees, wherein the obtaining and using of aliases is permitted only to previously authorized users, and linking the alias with the person behind it is impossible at all times.

This paper has presented a solution to the problem of participation in a critical environment by using an advanced system of citizen participation that includes the appropriate mechanisms of security to allow for audit, while ensuring proper operation of the system in every phase, with a special emphasis on protecting citizens' freedom of speech.

The strength of the system is based on the use of open source

software as a measure to prevent hidden tasks that might harm users, on the use of advanced security mechanisms and the use of smart cards that perform the most critical operations internally in order to leave no trace of them in the computer systems used.

This research group is working on the development of a secure telematic platform to support scenarios of Digital Democracy on the basis of web technology (complete description in (Gómez et al. 2005b)). The next step of this project is the implementation of the system and pilot projects in several collectives, which will help to show that the requirements demanded by society are technically viable, and that such initiatives do not pose the choice of abandoning advances on the field of civil liberties.

References

Carracedo, J., 2004, Seguridad en redes telemáticas, McGraw-Hill, Madrid, Spain.

DEMOS (Delphi Mediation Online System), 2003. [http://www.demos-project.org/].

DUNES (Dialogic and Argumentative Negotiation Educational Software), 2005 [http://www. tessera.gr/dunes/index.php].

EURO-CITI (European Cities Platform for On-line Transaction Services), 2002 [http://www.euro-citi.org/].

Gilbert, C., 2003, The changing role of the citizen in the e-Governance & e-Democracy equation, Commonwealth Centre for e-Governance. [http://www.electronicgov.net/pubs/research_papers/cath/index.shtml]

Gómez, A., Pérez, E., Sánchez, S., Carracedo, J., Moreno, J. & Carracedo, J.D. 2005a, VOTESCRIPT: telematic voting system designed to enable final count verification. Paper presented to the International CollECTeR LatAm 2005, Chile, October.

Gómez, A., González, C., Sánchez, S., Pérez, E. & Moreno, J. 2005b, Architectural design for a Digital Democracy telematic platform. Paper presented to the International CollECTeR LatAm 2005, Chile, October.

Gómez, A., Pérez, E., Sánchez, S., Moreno, J. & González, C. 2005c, Diseño de un sistema avanzado de Democracia Digital garante de la

libertad de expresión. Paper presented to the 3th Congreso Iberoamericano de Seguridad Informática (CIBSI05), Chile, November.
Luehrs, R., Pavón, J. & Schneider M. 2003, DEMOS Tools for Online Discussion and Decision Making, in LNCS 2722, ed. Springer-Verlag Berlin Heidelberg, pp. 525–528.
Lyon, D., 2001, Surveillance Society, monitoring every day life, Open University Press, Buckingham.
WEBOCRACY (Web Technologies Supporting Direct Participation in Democratic Processes), 2004 [http://esprit.ekf.tuke.sk/webocracy/index.html].

13

The risk of public data availability on critical infrastructure protection

Roba Abbas

School of Information Technology and Computer Science, University of Wollongong

Abstract

This paper examines the threat of freely available information on critical infrastructure protection (CIP) efforts. Critical infrastructure are the services required to maintain the stability and security of a country, and comprise both physical and cyber infrastructures. These interdependent entities must be protected from natural disasters, accidental

errors, and deliberate attacks. The CIP process typically includes vulnerability assessment, risk assessment and risk management, and has been a global concern for many years; the concern now amplified in Australia due to a number of recent events such the 9/11 attacks, and the Bali bombings. The events have called into question the role of information and communication technologies (ICTs) in both preventing, and aiding such activities. ICTs, primarily the Internet, provide a means of gathering public data. Public data refers to 'sensitive but unclassified' information; that is, information that may not on its own appear harmful, but when compiled with other data can be truly revealing about an individual or critical infrastructure. The paper presents the risk of 'sensitive but unclassified' data being available in the public arena (on the CIP process). There is an evident need for increased awareness of this issue throughout Australia. Additionally, further research must be conducted into the topic, in an attempt to achieve a balance between providing data publicly and restricting access in the interest of national security.

Keywords: public data, information access, terrorism, critical infrastructure

1 Introduction

This paper examines the risk of freely available information on critical infrastructure protection (CIP) efforts. To establish a proper understanding of this subject, it is important to consider three fields of study. The areas to be independently assessed include critical infrastructure (a definition of the term, and why critical infrastructures are important), critical infrastructure protection (the steps in the protection process, and the impact of recent events), and public data availability (the nature of public data, the impact of information and communication technologies, and national security vs. open information access issues).

2 Critical infrastructure

Critical, by definition, refers to an entity that is essential or vital in nature (Bezerra et al., 2005). Critical infrastructures, more specifically, are the essential services that contribute to the stability and security of a country (Chakrabarty and Mendonca, 2004; Rinaldi et al., 2001).

From a historical perspective, critical services have been in existence since the development and growth of cities, which led to the need for water supplies (Mendonca et al., 2004). In the Australian context, critical infrastructure encompasses banking and finance, transport and

distribution, energy, utilities, health, the food supply and communications (Attorney General's Department, 2006; TISN, 2006). Throughout this paper, the term critical infrastructure represents the listed services.

In terms of the Australian situation, the Australian Security Intelligence Organisation (ASIO) provides a definition of critical services as:

> "[t]hose physical facilities, supply chains, information technologies and communications networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security" (ASIO, 2006).

This definition is reflected in key Australian agencies that focus on critical infrastructures, and related protection campaigns such as the Attorney General's Department and the Trusted Information Sharing Network.

2.1 Physical and cyber infrastructures

While critical infrastructure was traditionally described as the necessary physical services within a given community, the definition has been extended by a number of academics to encompass cyber infrastructures (Kun, 2002; Neumann, 2002; Overill, 2001). This is primarily due to the prominence of information and communication technologies (ICTs) in recent years, and the consequent increased reliance on computer networks.

De Bruijne (2004), and Chakrabarti and Manimaran (2002), state that the progression of information and communication technologies has created a situation where physical critical infrastructures heavily depend on the support and operation of cyber infrastructures. Similarly, Overill (2001) states that physical and cyber infrastructures are interdependent entities; in particular the prosperity of physical services such as power, water, electrical and emergency services is reliant on digital systems or infrastructures. These concepts are reinforced by Feglar and Levy (2004), who feel that computer communications underlie the global economy, and are required to ensure that physical infrastructures are properly functioning, as they are interrelated and interconnected.

2.2 Infrastructure interdependencies

In addition to the relationship between physical and cyber infrastructures, it is vital to consider the interdependencies existing between the individual infrastructures. These relationships are of particular importance, as critical infrastructures today do not exist in isolation; rather there are physical or logical connections between them. Mendonca et al. (2004) describe critical infrastructures as 'systems of systems'; that is, they must be regarded as interdependent services. While a number of studies (such as that by Rinaldi et al., 2001) model or map such interdependencies, Mendonca et al.'s investigation assesses the impact of such interdependencies in a real world situation (that is, the impact of interdependencies on the events of 9/11). The research revealed that disruptions were dispersed across all eight infrastructures (as recognised by the US President's Commission of Critical Infrastructure Protection).

Schainker et al. (2006) agree with this claim; that critical infrastructures should be viewed as inextricably linked entities. This is evidenced in the authors' study of the electricity infrastructure, which revealed that a threat affecting one area would undoubtedly impact on the dependent critical services. This is particularly relevant to aid in grasping the complex environment in which these services exist, and the difficulties in maintaining reliable operations, and protecting against potential vulnerabilities.

As is evident by this body of literature, critical infrastructure relationships are complex, and difficult to define and manage. Therefore, any study on critical services must consider such interdependencies, as they ultimately impact on the critical infrastructure protection process.

3 Critical infrastructure protection (CIP)

Critical infrastructure protection (CIP) refers to safeguarding the identified services from potential harm, including physical and/or electronic attacks (ASIO, 2006; Schainker et al., 2006). Amin (2005) and Mendonca et al. (2004) identify the sources of infrastructure vulnerabilities as natural disasters, system complexities, equipment failures, human errors and deliberate sabotage/attacks (which is the

focus of this paper). Similarly, Kun (2002) recognises these sources in view of national security, economic stability and public safety concerns, highlighting the importance of the infrastructure protection process.

The value of the CIP process is also evidenced in a number of recently established initiatives supported by government and research bodies within Australia, but also internationally. For instance, the Australian Research Council (ARC) lists critical infrastructure protection as one of the major 'Priority Areas for ARC Funding 2005-2006' (ARC, 2006). Additionally, issues of threat detection and counter terrorism (which can be considered subsets of the CIP process) are identified as essential by the Research Network for a Secure Australia (RNSA, 2006). This is also reflected in many nations, such as the US, which recognises critical infrastructure protection as one of its six mission areas (Yen, 2004).

Thus, the protection of critical infrastructure is a crucial issue for all countries, and chiefly aids in maintaining national security, an issue that has gained importance as a result of a number of events (particularly in recent history).

3.1 Recent events

CIP has been a global concern since the Cold War; however, the issue has gained increased exposure in Australia since the incidents of September 11, 2001 and Bali, 2002, in addition to the Y2K concerns of the late nineties (Rothery, 2005; Luiijf and Klaver, 2004; Emergency Management Australia, 2003; De Bruijne, 2004). Such recent events, specifically 9/11, have raised public awareness of the vulnerabilities and risks existing in their surroundings, and the need for eliminating or mitigating these threats (Neumann, 2002).

The CIP literature to date has a common element in that a majority of the studies cite these occurrences (that is, events of the past forty years) as creating a heightened need for protecting infrastructure networks (Amin, 2005; Amin 2002). Therefore, a situation presently exists where nations are developing the strategies and stages of the CIP process, in order to avert situations such as those identified.

3.2 The CIP process

As with the definition of critical infrastructures, the CIP process inevitably varies between nations. This process, whether referring to physical or cyber infrastructures, is constrained by a number of factors, such as social, political and economic aspects, in addition to a country's specific environment (Bezerra et al., 2005).

The first stage in the CIP process involves assessing the context in which the infrastructure exists (including consideration of the previously mentioned factors). A paper by Bezerra et al. (2005) suggests that a country's unique context affects the CIP strategies implemented, using Brazil's telecommunications infrastructure as a case example. This stage is followed by measuring the threats to the identified critical services, the establishment of security controls, the creation of an ideal scenario and finally a comparison with the actual situation (providing necessary recommendations).

Similarly, a study by Luiijf and Klaver (2004), deals with the various phases in the CIP process. They focus on the 'Quick-scan' phase, which identifies the critical assets that require protection. An essential outcome of this study is the need for a multi-tiered approach to CIP; that is, providing protection at the strategic, tactical and operational levels. Other authors (Jones et al., 2003) identify risk assessment (identifying the risks, sources, interdependencies and developing threat scenarios) and risk management (cost evaluation, and conducting a trade-off analysis when selecting a response option) as core phases of the CIP process, which follow the identification of the critical infrastructure.

Whilst CIP efforts are typically focussed on the protection of physical infrastructures, the importance of safeguarding cyber critical services is gaining recognition. Threats to cyber infrastructures can be just as damaging, and reach a greater population, as an attack may be perpetrated from across the globe, on multiple sites (Elbert, 2003). Feglar and Levy (2004) propose an independent process for protecting cyber critical infrastructures which includes scope definition, asset identification and valuation, threat and vulnerability assessment, risk analysis and risk management. Throughout the cyber protection process Shainker et al. (2006) state that an important element in maintaining cyber security is to understand that the infrastructure (as a whole) is only as secure as its

‘weakest link’. This also holds true for physical infrastructures, due to the interdependencies discussed in section 2.2. Additionally, the elements of the cyber protection process can be aligned with the physical CIP phases, as a general pattern in both models emerges.

For instance, Australia’s national guidelines for protecting both physical and cyber infrastructures involves risk assessments, public information and media management, prevention and preparedness, and response and recovery (Attorney General’s Department, 2006).

Although minor variations exist between the CIP phases internationally, the typical steps in the CIP process can be regarded as vulnerability assessment/scanning, risk assessment, and risk management (Luiijf and Klaver, 2004; Jones et al., 2003). This paper aims to introduce the potential risk posed by public data availability to the CIP process, an issue that has not been adequately addressed in the literature.

4 Public data availability

Public data is concerned with ‘sensitive but unclassified’ data that may be obtained through open or freely available outlets. This refers specifically to information that may be unclassified when used independently, but when combined enables inferences or previously unconsidered patterns to emerge, which may prove harmful to the CIP process (Thuraisingham, n.d.).

Givens (n.d.) states that public records (or data) may be provided in two ways, either freely or commercially. Even though the latter requires a fee for access, it remains available in the public arena and can potentially be obtained by all individuals.

Hariharan et al. (2005) extends the issue of data availability to focus on integrating geographic information system (GIS) data from disparate sources in order to improve the means in which data (particularly commercial) is accessed in CIP campaigns. This study marks a shift in focus from personal to geopatial data. For example, authors such as Givens (n.d.) focus on personal data, that is, information concerned with an individual, such as health and legal records. However, the focus of Hariharan et al.’s paper is on location specific data with regards to critical services.

Since the events of 9/11, a direct link has been drawn between data collection facilitated by information and communication technologies (ICTs) and the act of terrorism (Davies, 2002), or threats to critical infrastructure protection endeavours. The various aspects of ICTs in relation to CIP are examined.

4.1 The role of information and communication technologies (ICTs)

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 infrastructures (Popp et. al., 2004). These technologies provide outlets for data/information exchange, and have simplified the ability to transmit data.

ICTs are providing tremendous opportunities for development. Kun (2002) describes the traditional technology focus, which has been on increasing the capabilities, productivity, and increasing the speed of technology whilst concentrating on digitising data, information and knowledge. The author feels that technology users have also become more proficient in utilising the available technology tools, and consequently accessing information. This proficiency in technology use also applies to individuals with a malicious intent (such as terrorist groups, for example).

An introductory study into the consequences of public data availability on critical services (in the US) states that there is an increase in the education levels of the individuals/groups attempting to penetrate critical services (Breeding, 2003). Breeding's method involved assessing various online sources in an attempt to determine the threat posed by 'sensitive but unclassified' data availability to US physical security. The study found that terrorists' use of technologies, and the availability of certain tools, has become progressively sophisticated, allowing room for the collection, use and duplication of 'sensitive but unclassified' information, to be used for ill purposes. In a book titled Terror on the Internet: The New Arena, The New Challenges, Weinmann (2006) describes terrorist use of the Internet for information warfare (or cyber terrorism) purposes, and data collection.

Information warfare is closely related to the issue of cyber terrorism, a

term that was first used in the 1970s, but became popular in 1996. According to Overill (2001), the phrase is generally defined as the premeditated attack on information activities and infrastructures, whilst preventing an attack on one's own information resources. That is, information warfare involves employing both an offensive and defensive strategy simultaneously. This issue is particularly relevant due to the over-reliance on computer or cyber infrastructures, most notably the Internet. While authors such as Elbert (2003) feel that cyber terrorism is a recent, genuine concern for the protection of critical services, Weinmann suggests otherwise.

Weinmann's studies found that it is highly unlikely that terrorists will use ICTs to launch cyber attacks; however, the Internet remains a repository for the collection of information/data about transportation, infrastructures and maps, for example (Cherry, 2005). It is believed that terrorists are increasingly using ICTs to further their cause, and carry out their preparations (Davies, 2002). Furthermore, the "intelligence information gained by cyber terrorist activities can be used to support the more traditional forms of terrorism" (Elbert, 2003, p.16/17).

Relevant to this concept of data collection is the chief idea that information and communication technologies can both aid, and hinder national security efforts, with particular reference to terrorist threats (Kun, 2002). Authors such as Yen (2004), Popp et al. (2004), Stout (2004), and Amin (2005) provide some insight into these issues.

Yen (2004) examines how ICTs can be utilised positively to advance the homeland or national security cause. Popp (2004) also shares the view that if used to their full potential, ICTs can ultimately assist in making informed decisions, and potentially prevent terrorist attacks. However, it is also important to address the negative implications. That is, that these technologies are also at the heart of the national security problem, and may be utilised negatively.

Stout (2004, p. 142) describes the present age as a "hybrid era", in that it promises great potential for technological advancement within an uncertain context (referring primarily to terrorist activities). Technology was previously viewed in terms of its ability to provide safeguards, however, the theme of Stout's paper is that technology alone cannot prevent acts of terrorism, and data misuse. This is based on the premise

that information and communication technologies are revolutionising the area of communications, thus enabling improved information sharing, specifically through the use of the Internet. This signifies that the efficient and correct use, and understanding of these technologies will determine the success of both malicious activities, and national security operations (Stout, 2004).

Amin (2005) supports Stout's claims, classing the protection of critical infrastructures largely as a technological problem or issue. The author feels that technology can serve two purposes; the first is to aid in penetrating or threatening a particular infrastructure, the second to provide protection mechanisms to safeguard the same services.

The conflicting roles of ICTs have been widely discussed in the literature; resulting in the requirement to review a number of issues such as national security (including CIP) in terms of censorship, open information access, and the related privacy concerns.

4.2 National security (CIP), open information access and privacy

It has been asserted that the mentioned recent events (such as 9/11) could have been prevented if access to particular datasets in the public arena was limited (Kumagai, 2003). This accordingly raises the need for controlling access to 'sensitive but unclassified' data, in order to maintain national security. These concerns introduce the concept of censorship, or restricting access to information that may be used in an adverse manner. Davies (2002) notes that censorship in another era may have failed to be implemented or considered, as it attacks the basic principles underlying the right to privacy, free speech and open source information. However, it is now a current issue, which must be resolved or addressed. The literature on the censorship of ICTs, particularly the Internet, agree that this task is difficult to achieve, and somewhat impossible.

Peace (2003) explores the issue of censorship in higher learning institutions, such as universities, measuring the importance of this area to heads of computer services departments. The study suggests that the issue of censorship is not a priority at present, and will unlikely be one in the near future. Universities are in conflict in terms of restricting undesirable information, whilst allowing legitimate Internet sourced to be accessed. This struggle perhaps exists due to the nature of ICTs, and

particularly the Internet, which “defies censorship” because of its inherent structure, and characteristics, most notability its capacity to allow public access to information, and the creation and distribution of data (Ang and Nadarajan, 1996, p.74). These issues continue to be a topic of debate, with many views or solutions being offered by academics.

For instance, Shearer (1998) provides an alternative view to censorship, highlighting the need for establishing a ‘Code of Ethics’ to govern communications over the Internet. This is based on the need for the ‘responsible global citizen’ to overcome the negative aspects of Internet technology, requiring global community members to individually accept responsibility for their actions, and maintain basic human rights, environmental awareness, and global advancement. However, it must be noted that this paper was written in 1998, prior to a majority of the events discussed in section 3.1., after which the concept ‘public good’ has been generally disregarded in the literature. Instead, various governments, such as the Australian, have enacted technology-related (or censorship) legislation, such as the laws to intercept digital communications such as email.

While the discussion has focussed on censoring ICTs, a contradictory element exists in the literature, whereby there is the call for increased ‘intelligence’ or information access to assist with maintaining an appropriate level of national security. In recent years, government agencies have expressed the need for information or data collection in the interest of national security.

Kumagai (2003) stresses the need for information access, with a focus on the FBI (Federal Bureau of Investigation), and its role in intelligence gathering and counter terrorism. The FBI is seeking to reform in a number of areas of intelligence gathering, such as increased data warehousing and data mining; that is, collecting data on individuals from various data sources and identifying patterns. In collecting such data, Kun (2002) raises concerns over data misuse, and its impact on civil liberties. This raises the issue of balancing privacy concerns with national security issues.

Privacy literature and concerns have been in existence for centuries, however, such concerns have now been exacerbated, and personal privacy has been applied to the technology arena (Walters, 2001).

Givens (n.d.) discusses the delicate act of balancing access to public data and maintaining personal privacy, with particular reference to legal records (such as court files and case indexes). Governments are increasingly providing such information online. Givens (n.d.) feels that the notion of e-government (and data provision) is primarily to allow the public to monitor the activities of the government. However, a number of negative consequences will inevitably arise due to public record access, most notably that the records will be used for secondary purposes (such as to make inferences, and to perform data mining activities).

As this body of literature has suggested, balancing national security, open information access, and privacy concerns is difficult. Therefore, when identifying the threat of public data availability, it is important to note that providing mechanisms to counteract the threat is a difficult task, and must be carefully considered in the interest of Australia's national security.

5 Conclusion

This paper introduced the risk of public data availability on the critical infrastructure protection (CIP) process. This was achieved by amalgamating three bodies of literature including critical infrastructure, critical infrastructure protection and public data availability. The various factors surrounding and complicating the issue have been presented, raising the need for a detailed examination of the topic in terms of achieving a balance between public data access and maintaining national security in Australia. The awareness that freely available information can threaten the CIP process is a primary step in achieving this balance. However, it is very clear that further research into this field is required.

References

Adar, E. and Wuchner, A. (2005). Risk Management for Critical Infrastructure Protection (CIP) Challenges, Best Practices & Tools. *First IEEE International Workshop on Critical Infrastructure Protection*: 1-8.

Amin, M. (2005). 'Scanning the Technology: Energy Infrastructure

Defense Systems', *Proceedings of the IEEE,* 93(5): 861-875.

Amin, M. (2002). 'Security Challenges for the Electricity Infrastructure', *Supplement to Computer,* Security and Privacy 2002: 8-10.

Ang, P. H. and Nadarajan, B. (1996). 'Censorship and the Internet: A Singapore Perspective', *Communications of the ACM,* 39(6): 72-78.

ARC (2006). 'Priority Areas for ARC Funding' [Online], Available: www.arc.gov.au/grant_programs/ priority_areas.htm [Accessed March, 2006].

ASIO (2006). 'ASIO's Work: Critical Infrastructure Protection' [Online], Available: www.asio.gov.au/Work/Content/CIP.htm [Accessed January, 2006].

Attorney General's Department (2006). 'Australian Government- Attorney General's Department' [Online], Available: http://www.ag.gov.au/agd/WWW/TISNhome.nsf/Page/Current_Issues [Accessed March, 2006].

Bezerra, E. K., Nakamura, E. T. and Ribeiro, S. L. (2005). 'Critical Telecommunications Protection in Brazil', *Proceedings of the 2005 First IEEE International Workshop on Critical Infrastructure Protection,* The Computer Society.

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].

Chakrabarti, A. and Manimaran, G. (2002). 'Internet Infrastructure Security: A Taxonomy', *IEEE Network,* November/December 2002: 13- 21.

Chakrabarty, M. and Mendonca, D. (2004). Integrating Visual and Mathematical Models for the Management of Independent Critical Infarstructures. *IEEE International Conference on Systems, Man and Cybernetics*: 1179-1184.

Cherry, S. (2005). 'Resources: Terror Goes Online', *IEEE Spectrum,* January 2005: 72-73.

Davies, S. (2002). 'A Year After 9/11: Where Are We Now?', *Communications of the ACM,* 45(9): 35-39.

De Bruijne, M. L. C. (2004). 'Next Generation Critical Infrastructures: The Push and Pull to Real-Time', *2004 IEEE International Conference on Systems, Man and Cybernetics:* 4655-4661.

Elbert, A. J. (2003). 'Information Warfare: Are You at Risk?', *IEEE*

Technology and Society Magazine, Winter 2003/2004: 13-19.

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].

Feglar, T. and Levy, J. K. (2004). 'Protecting Cyber Critical Infrastructure (CCI): Integrating Information Security Analysis and Environmental Vulnerability Analysis', *International Engineering Management Conference 2004,* IEEE: 888-892.

Givens, B. (n.d.). 'Public Records on the Internet: The Privacy Dilemma' [Online], Available: www.privacyrights.org [Accessed March, 2006].

Hariharan, R., Shmueli-Scheuer, M., Li, C. and Mehrotra, S. (2005). 'Quality-Driven Approximate Methods for Integrating GIS Data', *GIS '05,* ACM, November 4-5: 97-104.

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.

Kumagai, J. (2003). 'Mission Impossible?', *IEEE Spectrum,* April 2003: 26-31.

Kun, L. G. (2002). 'Homeland Security: The Possible, Probable and Perils of Information Technology', *IEEE Engineering in Medicine and Biology,* September/October 2002: 28-33.

Luiijf, E. A. M. and Klaver, M. H. A (2004). Protecting a Nation's Critical Infrastructure: The First Steps. *IEEE International Conference on Systems, Man and Cybernetics*: 1185-1190.

Mendonca, D., Lee II, E. E. and Wallace, W. A. (2004). 'Impact of the 2001 World Trade Center Attack on Critical Interdependent Infrastructures', *2004 IEEE International Conference on Systems, Man and Cybernetics:* 4053-4058.

Neumann, P. G. (2002). 'Risks to the Public in Computers and Related Systems', *Software Engineering Notes,* 27(1): 7-17.

Overill, R. E. (2001). 'Information Warfare: Battles in Cyberspace', *Computing and Control Engineering Journal,* June 2001: 125-128.

Peace, G. (2003). 'Balancing Free Speech and Censorship: Academia's Response to the Internet', *Communications of the ACM,* 46(11): 105-109.

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 Analysing Critical Infrastructure Interdependencies. *Control Systems Magazine, IEEE* 21(6): 11-25.
RNSA (2006). 'Common Research Opportunity' [Online], Available: www.secureaustralia.org/Research/ ResearchAreas.php [Accessed March, 2006].
Rothery, M. (2005). 'Crticial Infrastructure Protection and the Role of Emergency Services', *The Australian Journal of Emergency Management*, 20(2): 45-50.
Schainker, R., Douglas, J. and Kropp, T. (2006). 'Electric Utility Responses to Grid Security Issues', *IEEE Power and Energy Magazine,* March/April 2006: 30-37.
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.

14

Perceived risk: human factors affecting ICT of critical infrastructure

Peter R Croll[12] and Hasmukh Morarji[1]

[1]Faculty of Information Technology, QUT, Brisbane, Australia

[2]CSIRO Flagship Fellow, E-Heath Research Centre, Brisbane, Australia

Abstract

The adoption of new Information and Communication Technologies (ICT) to support our critical infrastructure (CI) services introduces new risks. Healthcare is selected as an example where existing manual processes are increasingly being replaced by electronic records and procedures. The patients, as individuals, play an important role in supporting effective ICT solutions and hence require inclusion to any risk analysis conducted by the researchers for the health managers. This paper considers whether current models for risk assessment are adequate for addressing the risks as perceived by the general public. It proposes a revised approach that allows for inclusion of the perceived risks affecting ICT adoption. The value of using the perceived risk model with other public service critical infrastructures is discussed.

Keywords: risk assessment, perceived risk, privacy, electronic health data, critical infrastructure

1 Introduction

The continued adoption of Information and Communication Technologies (ICT) for use with critical infrastructure (CI) services introduces new risks. While some of these risks are associated with the technology itself, much is associated with new procedures and business practices. Whenever new ICTs are introduced, the aim is to achieve some improvement over the existing systems, although, more often in practice, the outcomes achieved do not always meet the original objectives (DCITA 2005). Our essential critical infrastructure will include services, such as the power utilities, water, health, government and defence. Management of these services will see the potential of ICT for realizing not only greater administrative efficiencies, but an emphasis wherever possible on *safety* and *quality*. The question often remains as to how well the management will understand and address the new risks that are associated with the changes introduced with ICT adoption.

It is widely recognized that, in practice, risks can be hard to quantify and will often involve attributes requiring qualitative and/or subjective measures. This stems from the need to calculate the probability of occurrence, which will require an estimate of the likelihood of future events. Hence, it is hard to have a high degree of confidence in the accuracy of any such estimates unless we are dealing with highly regular systems with an established history of past incidences and operating

within a known predictable environment. There are many applications that govern our critical infrastructure where this does not apply. A number of methods are well researched for investigating risk, e.g. CORAS, CRAMM with software tool support (Abie 2005). Regardless of the method or tool selected, it has to be recognized that each application has its own set of interconnected hazards and problems relating to its particular operating environment and unique set of external impacts.

This paper will focus on healthcare as critical infrastructure. This is an area that has a history of manual record keeping and hence does not necessarily have the luxury of hindsight for electronic system failures. Furthermore, it is an area where the public have a right of say (for example, consent over the use of personal data) and hence the perception of the individual has a strong influence on the behaviour. It follows that this paper will explore a model that details the interdependencies and relationships of risk management and the cycle required for risk minimization. The influence of the individual and how the perceived risks they possess is examined to determine where the cycle can be more effectively closed through directed training and education. Finally, the applicability towards other public service critical infrastructures and the need for further research are discussed.

2 Healthcare

Healthcare within Australia is a complex mix of private, public, state and federal provision. To date, most health data has been collected and stored as manual records but the move towards integrating the wealth of electronically stored health data continues to gain momentum in Australia and internationally. The need for continued investment in e-health is evident with the necessity to move from what has been a highly manual, diverse and widely distributed collection of health data to standardized, highly available and connected electronic record systems (Health Connect 2004, NeHTA 2005). The accumulation of disparate data sources across organizations and across various states and territories presents challenges for system integrators. They must address non-trivial issues of a technical, legal and operational nature. The potential rewards for integrating systems and linking health records are numerous. They

include not only administrative efficiencies and improved safety, but research into better treatments and outcomes from our understanding of patient journey, cohort studies, etc.

The superior high speed connectivity and remote access, realized through the adoption of information technology (IT), presents new and unforeseen problems. For example, the need to maintain confidentiality requires state-of-the-art in IT security technologies. The need to respect privacy requires policies and implementations that adhere to our complex legal framework in Australia. Failure to address adequately these issues will put the possibilities of further health data computerization difficult. For example, the inability to adequately reassure general practitioners of the trustworthiness of a proposed system was putting the planned introduction of the £6 Billion integrated National Health system project in the UK at risk of catastrophic failure (Medex 2005). The necessary trust can be fragile and easily broken through well publicized incidences. The need to understand and manage the risks and minimize their impact is therefore critical. For example, in healthcare the public have little knowledge of how their personal data is stored and accessed by others. In the main citizens rely on trust that the institutions and professionals involved will do what is necessary to maintain confidentiality of sensitive information. To date, there may not have been many incidences involving the leaking of medical data to unauthorized or inappropriate users and certainly not many incidences that have been well publicized (the exception to this of course is the US Watergate affair, yet most people know that this involved a physical break-in and not a computer hack).

2.1 e-Health risks

With the increased push towards national health data integration such as Health Connect (2004) and the problems of differing state and organizational policies, risks are far from static. The National e-Health Transition Authority states that privacy protection in Australia is a complex patchwork: “NeHTA’s position has been to chart health privacy requirements within the privacy environment that we have now. It is considered possible to navigate the existing privacy environment although this is not without some risk and may require future changes” (NeHTA 2005). Regardless of the guidelines there are some real risks to

collecting and using sensitive health data. These include the risks faced by data custodians in not following the privacy principles and their local policies, in particular, the disclosure of individuals and the incorrect use of data. Other risks include the loss of trust that the providers of data, i.e., the patients, have in the IT systems we use. That is, the ability to use patients' data for research without their consent is irrelevant if their trust is eroded and hence they do not participate in providing the necessary data (Croll and Hansen 2005).

The Health Insurance Portability and Accountability Act of 1996 (HIPPA), which has recently become a legal requirement in the US, is an attempt to reduce risks and protect the confidentiality and security of healthcare data by establishing and enforcing standards and by standardizing electronic data interchange. Although standards are an important move and something that Australia has endorsed through recent significant increased funding to NeHTA (2005), they emphasize what needs to be done but do not prescribe how to understand and minimize the various risks encountered..

3 Risk management cycles

There are a number of approaches available to minimize risk. Figure 1 shows a cycle of procedures that need to be followed for successful risk minimization. Risk is defined as the "Probability of Occurrence x Consequence" Note that the term "risk" is often used interchangeably with the following, Frequency of Events, Likelihood, Results, Impact, etc., to cater for different audiences, such as managers rather than technical personnel. The basic aim is to provide the best measurement or estimation for both these Probabilities and Consequence criteria from which the risk can be calculated. The resultant risk measure is often generalized into categories for easier consumption, e.g. Negligible, Low, Medium, High, and Extreme. If the risk is considered unacceptably 'High' or if it could easily be reduced, then risk minimization measures are implemented. There are two basic approaches: 1) avoid the risk; and 2) mitigate against it. In some cases the hazard causing the risk could be avoided by design and therefore effectively eliminated (e.g., removing human intervention with an operational system to avoid any human

errors). Alternatively, after detection of a hazard, mitigation techniques can be applied to reduce the likelihood of further harm (e.g., natural environmental hazards which may be unavoidable). Both approaches would require some changes in the system design or current work practices. This should have a positive effect on reducing the number of incidences and hence further analysis will show a reduced risk. This process can be repeated until the risk has been minimized to an acceptable level.

Figure 1. The Cycle of Calculated Risks and Work Practice Change

For many of the critical infrastructures the business managers and leaders can dictate how the general public should behave when interacting with their services. For example, in times of national emergency, in addition to any legal obligation, there is an expectation that the public will comply with the directions of defense forces and emergency services. This permits for some degree of predictability and allows the services to analyze the risks and provide the best response for differing circumstances. That is, they can specify changes in work practices, as shown in the cycle of figure 1, to facilitate risk minimization. Yet for some of our services this approach is neither practical nor productive. Furthermore, as citizens increasingly understand and exercise their rights, an individual's compliance cannot be guaranteed.

The importance of the human impact, when designing critical systems applications, is appreciated by ICT systems designers and software engineers. However, humans are individuals and do not necessarily respond in predictable ways. This implies that, for the purpose of risk analysis, we cannot regard individuals in the same way as machinery that can be reduced to simple mechanisms, such as Finite State Machines (Croll & Croll 2004).

In the case of Healthcare it would be important to appreciate the power of the media in shaping people's opinions. Although they may wish to ignore some of the facts for a good story line, the way the media often

reacts depends on what information they have at hand. The media tries to show the inadequacies of our systems by indicating that of those people responsible nobody seems to know anything or particularly care about a given problem or incident. An aim in healthcare services should be to ensure the public trust our ICT systems to reduce the risk of noncompliance. This can be addressed by ensuring that the media is provided with prompt and comprehensible assurances following an incident. The experience of the authors' interviews with healthcare IT services shows a mixed reaction with many data custodians not knowing who is responsible for reporting on an incident such as a security or privacy violation. This is an example where a perceived risk of insecure health record data is fuelled by the number of reported incidences yet the measures put in place to reassure the public are often inadequate. This has been the experience with Internet banking where perceived risk plays a crucial role (Kim & Montalto 2002).

4 Perceived risk

From the general public's perspective, the security of our health data is an example of a *perceived risk* (Dowling & Staelin1994). This is a risk based on opinion rather than one calculated or estimated from collected data. Perceived risks must be accounted for as they may have a direct influence on the consequences of a given hazard. That is, how people cooperate and act under different situations can determine the outcome (Solvic 1993).

Using the data from the *1998 Technology Survey*, Kim and Montalto (2002) examined the effect of perceived risk of personal privacy invasion on the use of online technology by consumers. A probability equation model is used to model the discrete choice of online use given cross-sectional variation in perceived risk. Consumers are assumed to vary in the extent to which they believe use of online technology poses a risk of personal privacy invasion, and to choose whether or not to use online technology, given their perceived risk of privacy invasion. The results from the study are consistent with the view that consumers' perceived risk influences their use of online technology. Specifically, perceived risk of privacy invasion significantly reduces the use of online

technology.

In a paper presented at the *2002 WSEAS International Conference on Information Security*, Gonzallez and Sa Wicka (2002) describe a project which aims at understanding better the role of human factors in information security. It highlights the importance of a sound management policy in accordance to human nature. The problem requires an interdisciplinary approach involving relevant knowledge from technology, information science, psychology and management

The relationship between health, foreign policy, and security are examined in a programme supported by the Nuffield Trust and funded by the Nuffield Health and Social Services Fund, UK (Innes 2005). It is based on the recognition that health has become a major international political issue cutting across traditional policy and academic communities.

In his paper on bio-terrorism, Professor Michael Dando, a Professor of International Security and Director of Bradford Weapons of Mass Destruction Disarmament Research Centre, argues that biological agents not only pre-dated the terrorist attacks of September 11 and the anthrax attacks, but had been used in the 1990s by both state and non-state actors as weapons of terror. September 11 and the anthrax letters however increased the perception of risk.

Richard Smith, editor of the *British Medical Journal* notes that although World Health Organisation emerged as an authoritative and trusted voice on Severe Acute Respiratory Syndrome (SARS), the overwhelming impression is one of scientific uncertainty creating the conditions whereby a sense of vulnerability could emerge. The initial fears of the public health community that SARS might have been the harbinger of a new global flu pandemic revealed the tendency towards worst case thinking, while the manner in which rumour and suspicion flourished whenever hard information was lacking indicated the potency of opinion- people were willing to listen and believe rumour and opinion rather than wait for expert assessment. With SARS, for example, what was crucial in explaining the popular reaction was the perception of increased risk.

Speaking at an international conference entitled *Risk Perception: Science, Public Debate and Policy Making*, David Byrne, Commissioner for Health and Consumer Protection for EU, made the following observation:

> "Unfortunately, because of the inconsistencies and contradictions in how the public perceives risk, all our efforts may not be enough. If we fail to make progress [in understanding risk perception], there is a very real danger that an "anti-science" agenda may take root in European society – leading to a society hampered and restricted by a collective neurosis, lacking in self confidence, resistant to innovation and unwilling to embrace change. We must not be deluded by the sometimes seductive, yet false, notion of a zero risk society," said Commissioner Byrne (Consumer Voice, Special Edition, March 2004).

Also speaking at the same conference, *Risk Perception: Science, Public Debate and Policy Making*, Professor Ortwin Renn from the University of Stuttgart made the following comments on perception of risk and socio-psychological models:

> "Perceptions have a reality of their own. Just like the characters in animated films who, suspended in mid-air, do not plunge to the ground until they realize their predicament, people construct their own reality and evaluate risks according to their subjective perceptions. Intuitive risk perception is based on how information on the source of a risk is communicated, the psychological mechanisms for processing uncertainty, and earlier experience of threats. This mental process results in perceived risk– a collection of notions that people form on risk sources relative to the information available to them and their basic common sense. Human behaviour is fuelled by perceptions not the "facts" or what scientists pose as "real" risks."

Research on risk perception has identified a range of perception models used by society in perceiving and assessing risk. Looking specifically at technological and natural hazards, the following perception models can be identified:

- Risk as a fatal threat (for this what probability plays hardly any role)
- Risk as fate (seen as beyond man's control)
- Risk as a personal thrill (seen as a test of strength, triumph over natural forces)
- Risk as a game of chance (probability of rare events are underestimated)
- Risk as an early warning indicator (scientist being obliged to report).

4.1 Model for perceived risk

As already discussed, the risk associated with human involvement may

be a perceived risk. That is, any calculation of risk has been based on evidence at hand, that may be incomplete, inaccurate, subject to prejudice, fears or beliefs. This presents two key problems for the risk minimization procedure. First, there is no consensus from a panel of experts but a range of opinions and ad-hoc judgments being made. Second, the techniques used for changing the system and work practices may not succeed in practice as the general public is not part of a professional workforce who can be dictated to by company policies (the exception here may be the defense and emergency services). Figure 2 shows how the risk minimization cycle can be modified to accommodate the perceived risks brought about by the human involvement. What the figure shows is that in order to modify the behaviour (which is critical for minimizing the perception of the risk), the outcomes need to be targeted at those aspects that will have the most influence. These are identified as 'Critical Factors'.

Avoidance is one of the risk control strategies mentioned above that attempts to prevent the exploitation of the vulnerability, and it seeks to avoid risk rather than deal with it after it has been realized, i.e., mitigated against. Avoidance could be accomplished through application of training and education. This creates a safer and more controlled organizational environment to achieve the necessary changes to end-user behaviour.

Figure 2. The Cycle of Perceived Risks and Critical Factors

5 Further work and conclusions

This paper reported on a study undertaken into the risk models that can be adopted for addressing ICT adoption with critical infrastructure services. Although healthcare was used as the case study it is considered applicable to other services where the human factors can have a significant effect on the outcome. For example, with the heightened concern over terrorism, the emergency services and armed forces need the public support for effective detection prior to an incident. The perceived risk that the public may have towards revealing too much information may have a detrimental effect on the value of an IT system

used to monitor such incidences.

The perceived risk model presented (figure 2) shows a direct correspondence between the standardized calculated risk approaches (figure 1). Further research is needed to find a universal approach to dealing with varying knowledge of calculated and perceived risk. It is envisaged that this would be superior to handling these issues separately and allow for the experts to suggest viable outcomes to modify behaviour both in the workplace and with the public at large.

References

Habtamu Abie (2005) Risk Analysis, Risk Assessment, Risk Management, http://www.nr.no/~abie/ RiskAnalysis.htm, accessed Dec 05.

Consumer Voice, *Special Edition,* March 2004, Newsletter on food safety, health and consumer policy

P Croll and J Croll (2004) Q.U.i.P.S. a Quality Model for Investigating Risk Exposure in e-Health Systems, Medinfo Journal, ISSN: 1569-6332, Vol. 2004, 1023-7.

PR Croll and D Hansen (2005) Sharing Health Data: Privacy & Trust, Proceedings of the ICT Conference, ICT Centre CSIRO, ISBN 0 643 09277 3, Sydney, Nov.

DCITA (2005) Achieving Value from ICT: Key Management Strategies, Report by ANU and Opticon for the Australian Government's Department of Communications, Information Technology and the Arts, www.dcita.gov.au.

G Dowling, R Staelin (1994) A Model of Perceived Risk and Intended Risk-Handling Activity, *Journal of Consumer Research,* Vol 21 (1), Jun pp 119-134.

Gonzallez and Sa Wicka (2002) *A Framework for Human Factors in Information Security*, Jose J Gonzalez and Agata Sa Wicka, WSEAS Int. Conf. on Information Security, Rio de Janeiro, 2002.

Health Connect (2004) Fact Sheet – HealthConnect, www.healthconnect.gov.au/about/Fact.htm September, 2005.

Innes (2005) *Health Security and the Risk Society*, Professor Colin Mc Innes, University of Wales Aberystwyth, UK Global Health Programme.

Kim and Montalto (2002) *Perceived Risk of Privacy Invasion and Use of Online Technology by Consumers*, Sora Kim and Catherine P. Montalto, Vol 48, Consumer Interests Annual .

K Kim, B Prabhakar Initial Trust, Perceived Risk and the Adoption of Internet Banking, Internet Banking, pp 537-543.

Medix (2005) Medix UK plc survey (Q647) of doctors' views about the National Programme for IT (NPfIT), commissioned by Computer Weekly and The Guardian.

NEHTA (2005) The National E-Health Transition Authority, www.nehta.gov.au accessed Sept 2005.

P Solvic (1993) Perceived Risk, Trust and Democracy, Risk Analysis Journal, vol 13 (6), pp 675-682.

15

Conceptualisation of terrorism in modelling tools: critical reflexive approach

Lucy Resnyansky

Research Scientist, Defence Science and Technology Organisation

Abstract

This paper outlines a critical reflexive approach to an assessment of modelling/simulation tools. The concepts of terrorism and terrorism threat in modelling literature are analysed and compared with the contesting definitions of terrorism in political science and counter-terrorism discourse. Possible social implications of using particular concepts of terrorism and terrorism threat are identified. This study discusses how modellers provide better support to counter-terrorism analysis and decision making, by taking the above-mentioned approach.

Keywords: terrorism, threat, modelling, critical reflexive approach, sociology of science, social informatics

> Terrorism has been situated – and thereby implicitly also defined – in various contexts such as crime, politics, war, propaganda and religion. Depending on what framework one chooses, certain aspects of terrorism get exposed while others are placed 'outside the picture' if only one framework is utilised (Schmid 2004, p. 197).

1 Introduction

Modelling and simulation tools and techniques are used in such areas as research, intelligence analysis, decision-making, planning, and training (Barros & Proença 2005; Chittester & Haimes 2004; Enders & Sandler 2005; Giboa 1981; Haimes & Horowitz 2004; Sloan, Kearney & Wise 1977; Zilinskas, Hope & North 2004). The use of such tools may have important social and political implications due to the fact that, as every other technology, they offer particular visions of phenomena and support certain strategies and actions. Therefore, the development of modelling tools has to involve an assessment of their potential effects on work practices, institutions, and society. Also, modellers need to explicitly and critically reflect upon the concepts of social phenomena that inform their research and development in order to assess the validity of their models (Turnley 2005).

The purpose of this paper is to develop a critical reflexive approach to an analysis of modelling and simulation tools for counter-terrorism analysis and decision making. This paper explores the concepts of terrorism and terrorism threat in modelling literature. These concepts are analysed in order to understand: What aspects of terrorism they highlight

and what aspects are not addressed? What ways of dealing with terrorism threat are supported?

2 Previous studies

This study draws upon social informatics, sociology of science, philosophy of technology, and social constructivist studies of technology as a social construct and a 'social actor' that may affect work practices and contribute to social changes (Bijker, Pinch & Hughes 1987; Cawson, Haddon & Miles 1995; Ellul 1964; Kling 1992; Resnyansky 2002; Robbin, Courtright & Davis 2004; Roszak 1986; Turkle 1997; van House 2004). Specifically, it draws upon studies of the role of different groups (media, government, and different research communities) in conceptualising terrorism (Reid 1993; Weinberg, Pedahzur & Hirsch-Hoefler 2004).

Reid (1993) explores the ways of researchers' influence upon the U.S. government's conceptualisation of terrorism and, ultimately, its political decisions. Reid identifies three groups of researchers according to their approach: 1) from question, 2) from data, and 3) from method (i.e. modelling). According to Reid, the first group has the biggest influence upon political decisions; the last group (modellers) has not been considered as a source of any specific concepts of terrorism. Weinberg et al. (2004) analyse how terrorism is conceptualised by academics in three terrorism journals and argue that since 1985, the conceptualisation of terrorism has shifted from the psychological toward political aspects of terrorism. They explore the contesting definitions provided by political scientists and psychologists while modellers are not even mentioned.

Both studies show that terrorism is a highly contested concept. However, they focus on the conceptualisation of terrorism in qualitative social research. In this paper, the purpose is to draw attention to the modelling community as yet another source of the concepts of terrorism.

3 The contested concepts of terrorism

There are a number of studies aiming to analyse the epistemological, practical, and social implications of using particular definitions of terrorism in political science, criminology, psychology, and sociology (Black 2004;

Hoffman 1998; Horgan 2005; Ganor 2005; Rosenfeld 2004). The definitions are analysed in order to understand whether they facilitate an observation of the phenomenon; whether they enable researchers to discriminate between different types of politically driven violent activities (terrorism, guerrilla warfare); and whether they help provide a legal basis for the implementation of force and security measures (Schmid 2004).

In political science, terrorism is defined in relation to the category of violence. The definitions of terrorism as a form of violence enable researchers to conceptualise terrorism as behaviour, as a form of coercive, violent communication (Crelinsten 1998). More detailed and contextually-specific definitions of terrorism as a form of political violence include the identification of its specific motives and causes (criminal activity, political conflict, or war), the perpetrator (political criminals, insurgents, or state actors), and the target (political actors, casual targets) (Schmid 2004). According to a study of definitions of terrorism in three scientific journals, threat is just one of the aspects of the meaning of terrorism, and not always a necessary one: “[t]errorism is a politically motivated tactic involving the threat or use of force or violence in which pursuit of publicity plays a significant role” (Weinberg et al 2004, p. 782).

In contemporary counter-terrorism discourse, however, there is a trend to define terrorism in relation to the category of threat. One of the consequences is the extension of the area of counter-terrorism to such phenomena as drug trafficking, IT security, organised crime, illegal immigration, and infectious diseases (Crelinsten 1998). As Crelisten argues, the conceptual blurring of crime and terrorism, and the resultant blurring of internal and external policing and national and societal security, have serious implications for liberal democracies (the rule of law, accountability, openness and public trust, and confidence in the government).

The adoption of the military concept of threat results in the proliferation of an ontological metaphor of terrorism. The ontological metaphor is a way of “viewing events, activities, emotions, ideas, etc., as entities and substances” (Lakoff & Johnson 1980, p. 25). On the one hand, ontological metaphors are useful because they allow people to quantify their experience, identify a particular aspect of it, consider it as a cause, act with respect to it, etc. For example, the conceptualisation of terrorism as an

entity enables researchers and practitioners to focus on the intent of the threatening agent, the probability of this threat becoming a reality, as well as on its capability to inflict human loss and damages to property. On the other hand, the conceptualisation of terrorism as an entity may contribute to the perception of terrorism as a threatening agent similar to such threatening agents as foreign states. This perception may result in silencing the psychological and moral aspects of terrorism. Terrorism research and counter-terrorism efforts are then re-directed away from an analysis of individual terrorists' sociological and psychological profiles and motivations towards such issues as terrorism as a new/old threat, or the life cycle of terrorism (Tucker 2001). Also, such a conceptualisation of terrorism highlights societies and economies, rather than individuals, as the primary targets of terrorism:

> What should we conclude finally about the threat posed by the supposed new terrorism? It is possible that terrorists could get hold of a CBRN weapon and devastate a city. Without minimizing the damage this would do, especially the possible political damage, we must conclude that this is not the greatest threat posed by terrorism. The economies and societies of the industrial countries are wealthy enough, networked sufficiently, and their political life principled and resilient enough to survive such an attack. As far as terrorism is concerned, what has always posed the greatest threat is the shrewd and ruthless use of terrorism in the service of a strategically significant objective contrary to the interests of the target country or government, especially when this kind of terrorism has had the backing of an equally clever and ruthless state authority. From this perspective, the lethality of a group is not critical. Neither is it critical whether a particular group is networked or hierarchical or composed of amateurs or professionals (Tucker 2001, p. 12).

Many researchers find this omission of the individual and moral dimensions of terrorism to be problematic (*Threat Anticipation* 2005). Nonetheless, the conceptualisation of terrorism as a threatening agent still allows researchers and practitioners to focus on the agent of the violent activity and analyse its attributes. For example, the structure of terrorist organisations can be analysed, even though different conclusions regarding particular attributes' relevance may be made by different researchers. In addition, the use of this concept in political

science is embedded in multifaceted qualitative studies of terrorism as a specific historical and sociocultural phenomenon, where terrorism is studied as an activity or modus operandi. However, the fact that the modelling community is becoming more actively involved in terrorism research may change the balance and cause a proliferation of the concept of threat in counter-terrorism discourse. It is useful to understand how this trend may contribute to the re-conceptualisation of terrorism.

4 Concepts of terrorism threat in modelling literature

This paper emphasises modelling literature that uses economic and engineering approaches to assess the catastrophe/hazard risk and system vulnerability. For example, Coffin (2005) uses measurements made by a catastrophe risk modelling firm in order to predict the threat of terrorism to the U.S and other countries. The risk of terrorism is calculated on the basis of such measurements as the number of attacks and their severity (fatality and casualty rate). Chittester and Haimes (2004) assess the vulnerability of IT-based controls and equipment. Haimes & Horowitz (2004) develop a modelling game for tracking terrorist scenarios, which aims to support intelligence gathering and analysis for countering terrorism. This modelling game deals mainly with vulnerability issues. Zilinskas, Hope and North (2004) discuss quantitative models of bioterrorism risk assessment and argue that these models can help develop credible attack scenarios. Major (2002) develops a mathematical model for evaluating terrorism risk; terrorism risk is compared with a catastrophe risk.

Such models draw upon an abstract concept of threat, defined as a potential adversarial intent to cause harm or damage by changing the states of the system: "*Threat* is a potential intent to cause harm or damage to the system by adversely changing its states. A *threat* to a *vulnerable* system with adverse effects results in *risk*" (Haimes & Horowitz 2004, p. 9). The adoption of this abstract concept of threat may result in focusing on the target of the terrorist attack rather than on the attacker, and on the issues and problems related to protection measures, for example, the agents' incentive to adopt risk-reducing measures and to invest in protection (Heal & Kunreuther 2005; Lyon 2003).

The increasing interest in modelling the economic consequences of terrorist attacks may be explained by the fact that in November 2002, the U.S. Senate passed the Terrorism Risk Insurance Act that requires all commercial property and casualty insurers to cover losses due to international terrorist activity within the U.S. The insurers were forced to make difficult pricing decisions regarding terrorism risk, and "modelling companies are consequently bracing themselves for an upsurge in business" (Lyon 2003, p. 26).

The risk assessment and risk management models seem to be quite appropriate for providing solutions to such problems as infrastructure protection and the provision of a cost-benefit analysis of terrorism counter measures, as is practiced in risk management applied to other hazards (Clarke 2004). It is, however, useful to be aware that this perspective is more *reactive* than *proactive* and, therefore, orientates towards living with terrorism threat rather than towards its anticipation and elimination. It may also be suggested that such models have a rather narrow area of application in the practices of counter-terrorism agencies aiming at the prevention of terrorism and the anticipation of terrorism threat.

Although these models measure the effects of terrorism in terms of casualties and damages, they do not aim (and are unable) to take into consideration the social, cultural, political, and moral aspects of these effects. In fact, the conceptualisation of terrorism as a factor/cause of economic loss silences the moral aspects of terrorism. Instead, it promotes a perception of terrorism as a catastrophe or a disaster whose consequences need to be priced. Therefore, the conceptualisation of terrorism threat as yet another hazard (or a factor influencing a consumer's choice) may contribute to the naturalisation of terrorism. This, in turn, may be considered as a defeat of liberal democracies in the *war on terror*.

On the operational level, the use of the models shaped by abstract concepts of risk and threat also may have serious social implications. For example, there are quite sophisticated and reliable methods of risk assessment developed within systems engineering. However, one must be very cautious about using these methods in such areas as, for instance, security checks, because the development of rigorous models for the assessment of the risk that a person seeking entry into a country

may pose, requires that a correlation is established between the sociological categorisation used for individuals' profiling and their commitment to terrorism. However, as Testas (2004) notes, quantitative models that are not supported by qualitative studies of specific contexts may be misleading in regard to the real causes of certain people being involved in terrorist activity. Also, the application of models which may result in labelling individuals as potential terrorists simply on the basis of statistical correlations, often grounded within uncertain data (Horgan 2005), seems to be in conflict with the basic human rights and democratic values.

5 Conclusion

This preliminary analysis suggests that the current modelling literature highlights the catastrophe-centred concept of terrorism. In terms of its implications, the adoption of this concept may be misleading in regard to the causes of the terrorism threat emergence as well as individuals' involvement in terrorism activity; it may encourage security agencies (and the society in general) to adopt a reactive rather than a proactive position in relation to certain threats; and it may also contribute to the naturalisation of terrorism. In order to provide a balance to this concept of terrorism, it is necessary to employ a wider range of methods and approaches within modelling and simulation.

This paper also suggests that the analysis of the rigorous methods and techniques is only one aspect of the assessment of the modelling/simulation tools. This assessment also requires a critical reflexion upon the operational and social implications of the concepts offered together with these tools. These concepts may affect the users' practices if they are accepted uncritically. Therefore, the analyses of the concepts which inform simulation and modelling can help the modellers assess existing methods/models in terms of their suitability for particular purposes and practices and provide a better guidance to the user regarding the modelling/simulation tools' capability.

References

Barros, CP & Proença, I 2005, 'Mixed logit estimation of radical Islamic terrorism in Europe and North America: A comparative study', *Journal of Conflict Resolution,* vol. 49, no. 2, pp. 298-314.

Bijker, W, Pinch, T & Hughes, T 1987, *The social construction of technological systems: New directions in the sociology and history of technology*, MIT Press, Cambridge, MA.

Black, D 2004, 'Terrorism as social control', in *Terrorism and counter-terrorism: Criminological perspectives*. *Sociology of crime, law and deviance: Vol* 5, ed. M Deflem, Elsevier, Amsterdam.

Cawson, A, Haddon, L & Miles, I 1995, *The shape of things to consume: Delivering information technology into the home*, Avebury, Aldershot, UK.

Chittester, CG & Haimes, YY 2004, 'Risks of terrorism to information technology and critical interdependent infrastructures', *Journal of Homeland Security & Emergency Management*, vol. 1, no. 4, pp. 1-20.

Clarke, MC 2004, 'Terrorism, engineering and the environment: their interrelationships', *Terrorism and Political Violence*, vol. 16, no. 2, pp. 294-304.

Coffin, B 2005, 'Terrorism in 2005', *Risk Management,* vol. 52, no. 1, pp. 34-39.

Crelinsten, RD 1998, 'The discourse and practice of counter-terrorism in liberal democracies', *Australian Journal of Politics and History*, vol. 44, no. 1, pp. 389-413.

Ellul, J 1964, *The technological society*, trans. J Wilkinson, Vintage Books, New York.

Enders, W & Sandler, T 2005, 'Transnational terrorism 1968-2000: Thresholds, persistence, and forecasts', *Southern Economic Journal*, vol. 71, no. 3, pp. 467-482.

Ganor, B 2005, *The counter-terrorism puzzle: A guide for decision makers*, Transaction Publishers, New Brunswick U.S.A.

Giboa, E 1981, 'The use of simulation in combating terrorism', *Terrorism,* vol. 5, no. 3, pp. 265-280.

Haimes, YY & Horowitz, BM 2004, 'Adaptive two-player hierarchical holographic modelling game for counterterrorism intelligence

analysis', *Journal of Homeland Security and Emergency Management,* vol. 1, no. 3, pp. 1-21.

Heal, G & Kunreuther, H 2005, 'IDS models of airline security', *Journal of Conflict Resolution,* vol. 49, no. 2, pp. 201-217.

Hoffman, B 1998, *Inside terrorism*, Columbia University Press, London.

Horgan, J 2005, *The psychology of terrorism*, Routledge, London.

Kling, R 1992, 'Audiences, narratives, and human values in social studies of technology', *Science, Technology & Human Values,* vol. 17, pp. 349-365.

Lakoff, G & Johnson, M 1980, *Metaphors we live by*, The University of Chicago Press, Chicago.

Lyon, P 2003, 'Modelling the unthinkable', *Risk,* vol. 16, no. 3, pp. 26-28.

Major, JA 2002, 'Advanced techniques for modelling terrorism risk', *Journal of Risk Finance,* vol. 4, no. 1, pp. 15-25.

Reid, EOF 1993, 'Terrorism research and the diffusion of ideas', *Knowledge & Policy,* vol. 6, no. 1, pp. 17-38.

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, viewed 30 September 2003, <http://www.education.unisa.edu.au/JEE>.

Robbin, A, Courtright, C & Davis, L 2004, 'ICTs and political life', in *Annual review of information science and technology*, ed B Cronin, Information Today, Medford, NJ.

Rosenfeld, R 2004, 'Terrorism and criminology', in *Terrorism and counter-terrorism: Criminological perspectives*, ed. M Deflem, Elsevier, Amsterdam.

Roszak, T 1986, *The cult of information: The folklore of computers and the true art of thinking*, Pantheon Books, New York.

Schmid, AP 2004, 'Framework for conceptualising terrorism', *Terrorism and Political Violence,* vol.16, no. 2, pp. 197-221.

Sloan, S, Kearney, R & Wise, C 1977, 'Learning about terrorism: Analysis, simulations, and future directions', *Terrorism,* vol. 1, no. 1, pp. 315-329.

Testas, A 2004, 'Determinants of terrorism in the Muslim world: An empirical cross-sectional analysis', *Terrorism and Political Violence,* vol. 16, no. 2, pp. 253-273.

Threat anticipation: Social science methods and models 2005, The Joint Threat Anticipation Center Workshop, April 7-9, The University of Chicago, viewed 3 January 2006, <http://jtac.uchicago.edu/conferences/05/> .

Tucker, D 2001, 'What is new about the new terrorism and how dangerous is it?', *Terrorism and Political Violence,* vol. 13, no. 3, pp. 1-14.

Turkle, S 1997, 'Seeing through computers: Education in a culture of simulation', *The American Prospect,* vol. 8, no. 31, viewed 7 May 2001, <http://www.prospect.org/print/V8/31/turkle-s.html>.

Turnley, J 2005, *Validation issues in computational social simulation*, viewed 5 December 2005, <http://hcs.ucla.edu/lake-arrowhead-2005/HCS2005_JessicaTurnley2.pdf>.

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.

Weinberg, L, Pedahzur, A & Hirsch-Hoefler, S 2004, 'The challenges of conceptualizing terrorism', *Terrorism and Political Violence,* vol. 16, no. 4, pp. 777-794.

Zilinskas, RA, Hope, B & North, DW 2004, 'A discussion of findings and their possible implications from a workshop on bioterrorism threat assessment and risk management', Risk Analysis, vol. 24, no. 4, pp. 901-908.

16

Towards protecting critical infrastructure - the role of information security management in Australian universities

Lauren May and Tim Lane

Information Security Institute, Queensland University of Technology

Abstract

Universities constitute an important aspect in protecting critical infrastructure from several perspectives: they host a large number of diverse systems from both a business and academic viewpoint; they characterise a fertile platform for IT exploration and research; and finally, universities reflect and promote community standards through their practices, customs and processes. Within the context of a national strategy for securing cyberspace, security management in Australian universities tends to be challenged by the complexity of university culture and operating environments. In order to assist in securing university networks, this research proposes a security practitioner's management model. This model is aimed at facilitating the transition of security knowledge into actual implementation, with an end goal of an improved culture of compliance towards security in the university sector. This work is of significant value as to date there has been very little study into specific security management issues facing

Australian universities. This study highlights that future research would be well-placed to focus on benchmarking information security management within the university sector.

Keywords: security framework, security management, Australian universities, culture of compliance, information model

1 Introduction

Social order in contemporary society is highly dependent on accurate and predictable information structures. Internationally, boundaries in cyberspace necessitate an integral relationship between organisational structures and their information foundations. Australia is an active player in this global village. Consequently, maintaining continuity in modern organisations ultimately relies on the preservation of information. This is fundamentally achieved through the process of securing information in infrastructures.

All Australian industry sectors are dependent on infrastructure that they do not own or control (NOIE, 2002). The intention of this paper is to highlight issues with respect to maintaining the quality of the information in these infrastructures, focusing on the Australian tertiary sector. As a priority of national interest, the Commonwealth Government acknowledges the need to create a “culture of security” across all industry sectors, and acknowledges the need for “a greater focus on IT security in companies, including in outsourcing contracts, and for better communication within companies on security issues” (Richardson, 2002). In this context such a culture needs to be nurtured and practiced.

Universities provide the main source of our future leaders, innovators and technical workforce through their core business of teaching, learning and research (Luker and Petersen, 2003). The research interests of universities are fundamental to contemporary knowledge. As business organizations, universities are in a unique position to operate and contribute to the development of major global IT infrastructures. This activity places university communities in a strong supportive and leadership role for the nation in general with respect to safeguarding Australia through its critical infrastructures’ information systems.

2 Organisation/business information security

For any modern organization, effective operational control and strategic direction are dependent on the effective management of high quality information. In today's environment, universities are highly reliant on information to support their core activities and business operations. Universities depend on activities associated with creating, using and sharing information for teaching, learning and research functions. Add to this the extensive amount of intellectual property generated by universities, and the organisational importance of information and its security to universities is clearly evident.

It is therefore important to protect information in universities, a function achieved through effective information security practices. Information security ensures a high "quality of service" of information infrastructures and technologies, which support and complement the business goals of the organization. Having appropriate and effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is both integral and critical to the process of security management (Fulford and Doherty, 2003). The essential goals of information security then are much more than just "making sure nothing bad happens"- information security is increasingly associated with enabling the business function.

2.1 Threats in the tertiary sector

Universities constitute an important aspect in protecting national critical information infrastructures from several perspectives. At the institution level, three tangible issues predominate. First, universities host a large number of diverse systems, and act as Internet gateways for large numbers of systems. Securing these systems is not always approached with a structured or consistent process, particularly where Information Technology services are decentralised. This situation can provide a target rich environment for malicious code, as systems are often left ripe for exploitation and recruitment for cyber crime or targeted attacks on other systems. Large scale targeted attacks are growing, involving increased sophistication and organizations known as "bot" networks. Bot (short for robot) networks are "armies" of workstations that have been left exposed

to vulnerabilities, then “recruited” by hackers through mass dissemination and exploitation of malicious code. The compromised machines are controlled to carry out synchronized attacks and other malicious activity at the will of the attacker.

Second, university environments characterise a fertile “breeding ground” for IT exploration and research, attracting the interest of Internet hackers and even hackers from within the university community. An unmanaged environment can indirectly promote further development of hacking skills, tools and underground networks. Hacking incidents in American universities are well documented, with identity theft a prime target due to the use of social security numbers for student identification. In Australian universities, although the student identification numbers are not as useful for identify theft, targets can include a university’s finance, student, human resources and payroll systems, as well as any Internet facing systems.

Third, universities from an industry perspective are often a main source for future innovators and leaders (Luker and Petersen, 2003). From a community standing perspective, universities are in part reflected through their practices, customs and processes. This includes the extent to which safe computing is promoted and reflected within the security culture of the university, and the security culture that flows from the university sector to industry. Successful security implementations in higher education can also serve as guideposts or standards for related developments in the nation at large (Luker and Petersen, 2003). Any successful national response to the threat of cyber security needs to ensure that university networks and their information resources are protected. It also needs to ensure that their computing facilities are not used to launch attacks on critical infrastructure beyond the campus. The values of universities therefore ultimately reflect the values of the nation (Luker and Petersen, 2003).

2.2 Information security in the tertiary environment

Universities represent an eclectic environment containing an interesting challenge of cultures and technologies. The need to ensure academia is not impeded must be balanced against corporate and business requirements, against a backdrop of a transient and at times

explorative student base. This is often mixed in with a residential base, a research environment, broad core values, and a technology base consisting of multiple high bandwidth links to the Internet. Frequently a disparate mix of technologies, systems, operating environments and requirements is involved. The research environments in universities often have values including tolerance, individual autonomy and experimentation. These values contribute ultimately to developments in security, but paradoxically do not necessarily go hand-in-hand with fostering a culture of maintaining operational security (Luker and Petersen, 2003).

The function of information security management in universities operates necessarily between the corporate mandates associated with the business of providing education, and the cultural and pedagogical pursuit of academic teaching, learning and research. Dealing effectively with threats to information involves the process of information security management to ensure that overall risks, costs and efforts are properly balanced within the organisation.

Within the university sector, there is increasing acknowledgement of the importance of information security and its role in maintaining business continuity and social responsibility. Despite the increasing acknowledgement of the need for security, university members understandably differ in opinion on the application of specific practices and are therefore challenged with adopting the right balance between developing effective security measures and maintaining the fundamental principles of academia (Luker and Petersen, 2003).

Although information security in universities is a function that is often recognised as important, the priority allocated to security is not consistently commensurate with its perceived importance. This leads to difficulties and conflicts in understanding and agreeing on how security should be implemented and managed. Further, the often cited lack of a coordinated security approach tends to exacerbate the problem of gaining acceptance of security in a diversified and priority competing environment.

Few authors have recognized the fact that organisations not only have disparate security requirements, but that the dynamic business environments in which they operate are important factors that need to be

taken into account (Wood, 2002). The issue of why information security in the tertiary sector is any different to any other sector naturally arises. Higher education sectors in particular are unique in their semi privatized quasi government mode suggesting that establishment and implementation of stringent controls that would otherwise provide appropriate protection of information can in fact prove politically and technically difficult.

In the Educause book, 'Computer Network Security in Higher Education', Luker and Petersen (2003) discuss the principals of academic freedom in relation to strategies employable by universities for successful information security awareness and compliance. They also note the difficulties and challenges in this area. These authors suggest that achieving an acceptable security strategy can often result in conflict and challenges to achieving a balance between information security and the survival of academic freedom, or ingrained work practices (Luker and Petersen, 2003). It is necessary to carefully balance work practices with security control to make any headway, and in doing so to foster a culture of compliance.

3 A culture of compliance towards security

The New Oxford Short Dictionary on Historical Principles (1993) includes a definition of *culture* as "development of the mind, improvements through education and training". A *culture of compliance*, therefore, implies a culture whose participants harmonise towards a particular outcome. From a university perspective, a culture of compliance is inclusive of an awareness and understanding of, followed by compliance to, information security policies, processes and guidelines as part of the norms and values.

In this paper, compliance is based on the relationship between the university's security posture and the levels of compliance reflected at all levels of the university community through its culture. For universities to effectively incorporate information security into the routine of employees, it is necessary to change the information security culture of universities. In order to change the information security culture, each level of the organisation's behaviour needs to be considered to see how it affects the

organization (Vroom and Von Solms, 2004). This involves considering the organization from a layered and systemic approach for the purposes of cultural compliance.

3.1 The need for a systemic approach to managing security

Despite the importance of information security to Australian universities, existing approaches, standards and guidelines for security do not necessarily integrate well, and therefore do not provide a single point of understanding for how the process of information security should be managed. In determining how to achieve this, an analysis of the factors and issues that facilitate or impede the management of information security in Australian universities is required.

From an information security perspective the relatively unregulated environment in higher education institutions needs to take into account many contributing factors. Structural issues such as the size of the organization and the level of decentralization of Information Technology services and associated standards, policies and procedures affect the final security outcome. Business organisational issues such as the real cost of impeding 'academic freedom' through stringent security rules and requirements are always a concern. The fact that higher education sectors are a gateway to the Internet used by various stakeholders with conflicting interests affects the very basis of the organisation's approach to information security.

What is lacking in the literature is a systemic approach to the management of security in Australian universities; one which integrates and shows the relationship between the organisational context, behavioural aspects and a practical management model. A framework that satisfies two primary goals is needed. The first goal would allow university security practitioners to apply the management of information security in a more structured and cohesive manner. The second goal would be to increase the transparency and effectiveness of the security process towards organizational requirements. The research undertaken involves an exploratory analysis of key issues, some of which have been discussed previously in this paper. The main final objective of this research is to propose an integrated framework for information security management in Australian universities, an outline of which is given

towards the latter part of this paper.

From the security practitioner's perspective, an approach is required that provides a meaningful structure for progressing information security in an environment where competing priorities exist. An approach, underpinned by communication and awareness, should be focused on developing the organisation's culture of compliance. In this way, continuous security improvements applied through a framework that regulates the desired culture of compliance can be achieved.

Our proposed model aims to facilitate security management in the Australian university sector, by linking theories and findings from the study to an improved process for security management. The model provides a reference for security practitioners to understand how the process of security knowledge should be transitioned into implementation. Our proposed model is the culmination of our research in this area and the results of an exploratory survey of all Australian universities.

4 The survey

In order to improve on the current approach that universities adopt for information security management, a survey instrument was administered to all 38 Australian Vice Chancellor listed universities. The survey was aimed at gathering data central to the following three research questions.

1. What is the current status of information security management?
2. What are the key issues surrounding information security management?
3. How could information security management be improved?

4.1 Security practitioner's management model

A detailed analysis of the survey results gave rise to a proposal for a security practitioner's management model (see Figure 1). This model is designed specifically for university information security practitioners in Australian universities, whose role encompasses a responsibility for security implementation at the operational level. The structure of the model takes into account the fact that in many circumstances, universities struggle with a wide range of security best practices, frameworks and standards. What is often missing is a systemic approach to appropriately

implementing one or more standards. Key to the model is the challenge that cultural issues in universities often result in resistance to security, unless an effective method is considered.

Figure 1. Security Practitioner's Management Model

The model is designed to assist security practitioners to progress their institution's information security management programme. All too often, university security practitioners have an in-depth understanding or instinctive knowledge and feel for what should occur, but meet resistance or barriers to change, or simply encounter a lack of understanding of the need for change. The approach proposed in our model is therefore fundamentally different to simply implementing a set of controls based on a pre-defined standard. Our model attempts to describe an end goal of implementation; the "how" to implement rather than "what" to implement.

An important attribute of this model is the acknowledgement that best practices are recognized as playing an extremely important role in the management of security. In fact, a range of best practices is applicable to information security management within this model. This includes the growing maturity and consequent acceptance of well-regarded frameworks such as AS/NZS ISO 17799, CobiT, ITIL, COSO, ISO9002, Capability Maturity Model (CMM®), Systems and Security Business Architecture (SABSA), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (M_o_R®), and Project Management Body of Knowledge (PMBOK®) (IT Governance Institute,2005).

Although a selection of various elements of disparate best practices can be aligned to suit the organisation, invariably the use of best practices needs to be applied in context to organizational needs. The implementation of best practices tends to be costly and unfocused if treated as a purely technical guide. Implementation of best practices should be consistent with the organisation's business risk management and control framework (IT governance Institute, 2005). Therefore the most effective approach is to apply best practices starting at the business

context. An important distinction in this model which separates it from other models is the recognition that the application of technical controls is of little use without compliance to policy. Therefore not only is increased awareness required, but a culture of security must be developed to support the security programme. This requires clear policy with relevant work procedures, facilitated by a long term programme in which changes can be introduced in a manner that accounts for both work practices and security requirements (Gaunt, 2000).

The model leverages the SABSA (Systems and Security Business Architecture) method (Sherwood, Clark and Lynas, 2003) to provide a reference for facilitating the management process of security. Key to the model is the transitioning of knowledge into implementation, towards a culture of compliance. The model is premised on 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 are not enough; developing a culture of security is an end goal 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 17799 “Plan, Do, Check, Act (PDCA)” model, or another similar audit-based monitoring and corrective action process.

4.2 Process flow through the model

The model begins by feeding knowledge (gained from information security understanding, broader organizational 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 organization. Inappropriate application of security procedures can result in an expensive or unacceptable overhead (May, 2003). Therefore the interface ideally should be a structured and well accepted information

security management programme.

Table 1. Layers in the Security Practitioner's Management Model

Layer	**Description**	**Application**
Contextual Layer	The contextual layer is the business context of the organisation, incorporating the core business and organisational environment.	This layer essentially ensures that information security management is an enabler of the business by supporting the business and ensuring that security is aligned with the context and culture of the organisation.
Conceptual Layer	The conceptual layer represents the security posture of the organisation, reflected through the risk management approach and supporting policy.	The concepts and values of information security management are applied in this layer, providing the framework for security in lower layers.
Construct Layer	The construct layer symbolizes the virtual constructs of security, including logical security domains.	This is the logical application of security achieved through security design and architecture.
Physical Layer	The physical layer denotes the actual physical security including infrastructure, devices, hardware and software.	This is the application of security policy, architecture and design through physical means.

Operational Layer	The operational layer involves people and support mechanisms.	This is the human and procedural element, in support of security functionality.

The information security management programme then links into a layered structure which begins at the business strategic level, represented as the contextual level, and permeates throughout the organisation finishing at the operational layer (see Table 1). Across the layered structure, the process of communication and awareness facilitates the end byproduct, a culture of compliance. The central goal of the model is the required organizational level of a culture of compliance with the depicted external and internal influences viewed as inter- and intra-organizational factors impacting culture. The resulting compliance levels are then relayed 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.

4.3 Application of the model

This model is being applied at Southern Cross University in order to validate its applicability and usefulness. The model is core to the existing information security management programme in operation. (The existing programme predominantly uses the 17799 standard “Information Technology – Code of Practice for Information Security Management” (ISO/IEC 17799:2005) and uses the model to progress implementation).

5 Conclusion

The model provides an understanding of how to progress information security through an approach that is inclusive of any adopted best practices or standards. In summary, ensuring that the adopted information security management framework can be applied through a layered model across the enterprise is fundamental to ensuring a

structured, coordinated and comprehensive approach to information security management. This is regardless of which security standards are used.

This research work is of significant value to the university sector, as it represents a specific study into the security management issues facing Australian universities. It also provides an insightful examination on the current status of play, highlights issues and deficiencies, and provides a realistic recommendation on how improvements in security management can be made. The study recommends that future research would be well-placed to focus on benchmarking information security management within the university sector.

References

Fulford, H. and Doherty, N., (2003). "The Application of Information Security Policies in Large UK Based Organisations: An Exploratory Investigation. Information Management and Computer Security". Vol. 11, No. 3, pp. 106-114.

Gaunt, N., (2000). "Practical Approaches to Creating a Security Culture", International Journal of Medical Informatics, (6), 2000 151-157.

ISO/IEC 17799:2005. "Code of practice for information security management". ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Available at ANSI http://www.ansi.org/ Accessed 18 April 2006.

IT Governance Institute, (2005). "Aligning CobiT, ITIL and ISO 17799 for Business Benefit, 2005".

Luker, M. and Petersen, R., (2003). "Computer and Network Security in Higher Education". San Francisco, Jossey-Bass.

May, C., (2003). "Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy", Computer Fraud and Security, Volume 2003, Issue 5, May 2003, pp. 10-13.

National Office for information Economy, Business-Government Task Force on Critical Infrastructure (2002), "Information Security Awareness for Managers: What do they really need to know?" http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~NOIE+2.PDF/$file/NOIE+2.PDF Accessed

18 April 2006
Richardson, D., (2002). Speaking notes for the Director-General of Security at a Business/Government Task Force workshop “Critical Infrastructure Protection: a National Security Perspective” on 27/3/02 (http: //www.tisn.gov.au).
Sherwood, J., Clark, A., and Lynas, D., (2003). “Systems and Business Security Architecture”. Available at http://www.alctraining.com.au/pdf/SABSA_White_Paper.pdf Accessed 18 April 2006.
The New Oxford Short Dictionary on Historical Principles, (1993), Vol 1 A-M, Clarendon Press
Vroom, C. and Von Solms, R., (2004). “Towards Information Security Behavioural Compliance”, Computers and Security (2004) 23, pp.191-198.
Wood, C., (2002). “Information Security Policies Made Easy.” West Houston US, Pentasafe Security Technologies Inc.

17

Organisational factors and Australian IT professionals’ views of wireless network vulnerability assessments

Keir Dyce[1] and Mary Barrett[2 3]

[1] Centre for Computer Security Research, University of Wollongong

[2] School of Management and Marketing, University of Wollongong

Abstract

The paper reports on a survey-based study of Australian computer security professionals' use of and opinions about two types of wireless vulnerability assessment (WNVA): wireless monitoring and penetration testing. An initially surprising finding was how little both types are used, despite the ease with which wireless networks can be attacked, and the lack of clear obstacles to using them. In the light of aspects of organisational culture, including decision-making style and professional identity, the survey findings become more explicable. Senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organisation. 'Culture' may also explain why lack of time and expertise (rather than lack of financial resources), and senior management's discomfort with the idea of hacking into the network, mean neither wireless monitoring nor penetration testing is regularly used, even though wireless monitoring is fairly well understood. The paper also explores how aspects of organisational culture may limit the way even WNVA users go about the process, and how a cultural shift could help change users' perception about the risks and rewards of WNVAs. This could possibly threaten IT staff's professional identity, however, and this needs further research.

Keywords: organisational culture, wireless network vulnerability assessments, IT professionals, decision-making style, professional identity

3 Keir Dyce and Mary Barrett would like to acknowledge the assistance of Professor Jennifer Seberry, Director of the Centre for Computer Security Research at the University of Wollongong, who was the supervisor of the Honours project which led to this paper.

1 Introduction

This paper reports on a study of Australian IT professionals' use of and opinions about wireless network vulnerability assessments (WNVAs) and the organisational factors, especially culture, decision-making and professional identity, which may affect this. Protecting a business organisation's wireless networks presents a classic case of how a technically sophisticated, effective and therefore 'obvious' engineering approach to an important security problem can be undermined by not taking into account its social implications, both inside the organisations

where the solutions are implemented, and beyond them.

1.1 Wireless network security and organisational culture

For the very reason that the technical solutions to computer security issues appear simple and the need for them clear (at least to those who developed the solutions), their social implications may be difficult for others in the organisation to see, even IT staff. The concepts of organisational culture and especially subculture, that is, the accepted, often unspoken agreements and divisions in 'how we do things around here' go a fair way to explaining why such perceptual divisions are likely to occur and persist within organisations. We will consider culture and subculture from an internal perspective in more detail later in the paper.

Organisational culture is also impacted by the external environment. This has been shown at a broad level by Hofstede's (1980, 1991, 1993) well known studies of national differences in culture. Hofstede's work was undertaken by surveying more than 116,000 IBM employees in more than 40 countries about their work related values. Surveying employees of the same organisation in many countries allowed a variety of national differences in culture to be revealed. Within any one country, social implications of and attitudes towards computer security are likely to be affected by that country's culture. Case researchers such as Spurling (1995), who investigated how the Australian firm Alcoa promoted security awareness and overhauled its security systems, have found evidence suggesting this. Because of the link between external and internal aspects of organisational culture, even IT security professionals' views about computer security may be affected by the anxieties and ambivalences that surround computer security issues in the wider society.

1.2 Wireless networking, security risk and organisational culture

As we will see in more detail later, attitudes to risk are a typical part of an organisation's culture. Computer security risk is becoming an increasingly important issue, particularly as applications and uses of wireless network (WLANs) are continuing to develop rapidly in line with the equally rapid development of the 802.11 family of standards and amendments on which the vast majority of wireless networks are based.

WLANs enjoy high awareness and acceptance in organisations as they are now fast, cheap and easy to use compared with traditional wired networks. However Housley and Arbaugh (2003) comment that there is as yet a disturbingly low level of security for these networks, especially given that the very nature of wireless transmissions makes it easy to attack them. Specifically, it is easier both to intercept signals during transmission and to 'spoof' fraudulent messages on a wireless network compared to a wired network because the data travelling across a wireless network is transmitted to anyone capable of receiving within range of the signal. Security of information is of course of paramount importance to organisations which use wireless networks. If these networks are left vulnerable, organisations can suffer a whole range of consequences from the trivial and annoying to a potentially shattering organisational blow.

1.3 Two approaches to wireless network vulnerability assessment

Wireless network vulnerability assessment (WNVA) is the general term for methods of ensuring that wireless networks are as safe as possible. One kind, wireless monitoring, is a passive approach to testing security measures since it does not involve an attack on a network but rather gathers information about a network that could be put to use in the implementation of an attack – or would allow a network manager to determine if a network has any obvious security flaws. Depending on how it is used wireless monitoring could fall on either side of the boundary of legality or good ethics. Nevertheless a number of security professionals (eg Berghel 2004; Henning 2003; Tiller 2005) see it as an indispensable component in developing a secure wireless network.

A second, complementary approach to wireless network vulnerability assessment is penetration testing (penetration testing), which involves an active attempt to reach the wireless network to test how effective the security measures are in keeping unauthorised users and devices out of the network. It does not involve a full attack on the network, in which an 'attacker' attempts to copy or delete sensitive data and avoid being detected by those responsible for the network. It is a test to see if the wireless network's security measures can be penetrated, and the network accessed.

The issue of wireless security is well covered in a number of texts aimed at security professionals, for example Nichols and Lekkas (2002), Peltier *et al.* (2003) and Tiller (2005). Penetration testing in particular is well understood. However it is not known how widespread WNVA is within organisations. In addition, there is as yet no comprehensive framework outlining how to conduct a comprehensive WNVA. That is, there is no guide involving *both* wireless monitoring and penetration testing approaches which could help IT professionals identify the goals of a vulnerability assessment, prepare for the assessment, actually conduct it, analyse the results, and fix any security flaws that may have been identified. It would be useful to know whether IT professionals would find such a guide helpful. A prototype framework for a WNVA which reflects this lack of integration of the two approaches appears in Figure 1 overleaf.

2 Finding out IT professionals' use of and views about WNVAs

A study of what IT professionals actually do and think about WNVAs was conducted via a mail-out survey to members of the Information Security Interest Group (ISIG), an Australian organisation based in Sydney. The ISIG is a group of approximately 400 networking security professionals who were likely to have sole or shared responsibility for the management of one or more 802.11-based wireless networks. The study aimed to clarify some of the problems and unknown elements around IT professionals' use of WNVAs and their views on whether having a comprehensive framework for WNVAs would help them.

The survey contained both closed-ended and open-ended questions, giving respondents the opportunity to include additional information or opinion on specific issues. The study did not aim to link one variable causally with another, nor did it try to identify correlations between two or more variables, for example to try to connect views about WNVA issues with aspects of the IT professionals themselves or their organisations. Nevertheless the surprising nature of some of the results and the patterns in them suggest that some organisational factors, especially aspects of organisational culture and issues around IT professionals' identity, may have influenced the results. The results and discussion of these potential

organisational factors, are presented under the three main headings of the survey itself:

1. the extent of use of WNVAs, including either or both wireless monitoring and penetration testing,
2. how IT professionals used WNVAs, and
3. their opinions about the two approaches to WNVAs, and about aspects of vulnerability assessment frameworks.

Figure 1. Prototype vulnerability assessment framework

3 Results

3.1 Use of vulnerability assessments

A total of 62 useable survey responses were received. This appears a modest result, but given that the organisation consists of only about 400 members, the responses can be assumed to provide a reasonable view of the group whose views were sought.

Of the 62 respondents, only ten (16 percent) said they used wireless monitoring and three (5 percent) used penetration testing. This was a surprisingly low result, especially for wireless monitoring, which is widely known and publicised amongst IT professionals. The most common reason given in for not using wireless monitoring and penetration testing was that they were felt unnecessary. The second most common reason was a perceived lack of the necessary expertise for the two kinds of testing. Interestingly, lack of resources or other reasons were not perceived to be the problem.

3.1.1 Discussion: The possible role of organisational culture

When possible organisational factors are considered, however, especially organisational culture, it is less surprising that WNVAs have yet to find acceptance within organisations, even among IT professionals. Organisational culture encompasses such issues as the degree to which

employees are expected to pay attention to detail and to results, and be aggressive and competitive. It also includes the degree to which organisations are oriented around people's needs, rely on teams to organise work, and emphasise stability rather than growth (O'Reilly, Chatman & Caldwell 1991). An organisation's culture is known to be strongly influenced by senior management's style and preferences, the organisation's work and communication practices, reward structures, past history, power relationships, customer or user demands, accepted explanations of competitive pressures, and so on (Schein 1985). Culture serves as a powerful, practical and yet tacit way of organising management and employees' (including IT staff's) knowledge of the organisation's priorities and ways of operating.

Cultural values and assumptions, which are embedded at a deep level, sometimes remain when circumstances have changed, inhibiting the organisation's ability to respond to change. Thus earlier cultural norms about organisational security may outweigh IT professionals' judgements or even awareness of the need to revise standard security measures. We could predict, for example, that WNVAs would not be seen as necessary, since powerful organisational stakeholders including senior management, and even IT staff themselves, may still hold a traditional, 'wired network' view of their organisation, even though this is now more a part of history than reality. Many of the vulnerability assessment frameworks currently available are also based on the assumption that they will be applied in a wired rather than a wireless environment (Dyce 2005). This would tend to entrench the existing security norms of many organisations.

As the O'Reilly, Chatman & Caldwell (1991) formulation of cultural elements suggests, aspects of organisational culture strongly influence perceptions of what is important to organisational success. So culture also tends to dictate the choice of matters organisational members see as worthy of their time and effort. This may help explain why lack of time and expertise (rather than lack of financial resources), as well as senior management's discomfort with both the idea of hacking into the network, mean neither wireless monitoring nor penetration testing were regularly used.

3.1.2 Dominant cultures and subcultures

These explanations relate to views of the dominant organisational culture, generally the one espoused by senior management. However researchers on organisational culture such as Jermier *et al.* (1991) and Sackmann (1992) also point to the existence in most sizeable organisations of one or more subcultures which may or may not work in the same direction as the dominant organisational culture. Senior management, who as non-IT experts are unlikely to know much about the technical detail of WNVAs, may assume penetration testing involves hacking into the network, actually deleting data and then concealing the attack. IT security staff, by contrast, would most likely know that merely showing that a potential intruder could access the network is all penetration testing actually requires. If this is true, and it would be useful to undertake further research to establish the point, the dominant culture could be behind the lack of use of penetration testing.

By contrast, the IT subculture alone or in combination with the dominant culture may well be behind the non-use of wireless monitoring. As noted earlier, wireless monitoring can be used for illegal and/or unethical activity, such as monitoring which invades the privacy of employees or other parties. IT staff may therefore be concerned that using wireless monitoring may cause them as a group to be perceived by other organisational members as instigating inappropriate monitoring practices. Senior managers may be less concerned about this perception. After all many large organisations already monitor employees' web use and have told them this. However they may still be concerned about implementing new, possibly unpopular monitoring practices unless there is an overwhelming and demonstrated need to do so. In this case the dominant and the IT sub-culture may work together to discourage use of wireless monitoring.

3.2 How WNVAs are used

The answers to this section of the questionnaire broadly indicated that of the ten WNVA users in the sample, most had found that using either wireless monitoring or penetration testing or a combination of the two had proved valuable, in that network vulnerabilities had been revealed. A range of vulnerabilities had been both tested for and found, the latter

ranging from incorrect security configurations, rogue WAPs, overextended network boundaries and newly publicised vulnerabilities. A majority of those in the sample who used WNVA also indicated that one or other or both of wireless monitoring and penetration testing were part of the standard security procedures in their organisations. The results of a question about what practices are used as part of standard security procedure indicated that six of the ten WNVA users used just wireless monitoring, none used just penetration testing, and three used both. It was rare however to find that both wireless monitoring and penetration testing were used simultaneously in an organisation.

3.2.1 Discussion

In an earlier part of the results, thirty respondents or about half the sample said they believed a WNVA framework would help those who don't use either wireless monitoring or penetration testing due to lack of expertise. Moreover, the experience of WNVA users suggests that WNVAs are proving useful to organisations, and that users themselves recognise the value of making a WNVA a consistent procedure. The gap between the two findings – thirty respondents who believe a WNVA framework could be helpful for those who lack expertise, and only ten actual users – suggests that the lack of good WNVA frameworks may be preventing IT staff from implementing WNVAs. The next section explores this possibility further.

3.3 Practitioners' opinions about WNVAs including WNVA frameworks

In light of the findings about how WNVAs are used, it was surprising that practically all ten respondents who used WNVAs said they did not use a framework or a methodology to help them conduct security procedures. Three of the ten used a wireless monitoring framework; two of the ten used a penetration testing framework. Seven of the ten considered planning to be valuable as part of WNVAs, but only one had researched what approach to use. Very few used a framework (or knew where they could find one) for setting up, evaluating or refining a WNVA exercise. In addition, very few felt a WNVA should be done routinely after network changes, despite the fact that such changes may introduce

network vulnerabilities.

3.3.1 Discussion – the possible role of organisational decision-making style

IT professionals using WNVAs have found them useful and incorporated them into standard operating procedures. At first glance, this makes it surprising that very few IT professionals in this sample used of any framework to carry out a WNVA. However styles of organisational decision-making may explain this situation. Styles of decision-making, whether slow and considered, or fast and impulsive, also form part of culture. 'Planning' will fit with espoused values of rationality in most organisations' cultures, and also with cultures which are 'outcomes' rather than 'process' focussed. According to Simon (1979), however, in practice it is often impossible to explore planning options exhaustively because of time constraints and other limitations of the working environment. Instead, people typically use what he has called 'bounded' decision-making. That is, they make decisions on the base of limited research and choose from a reduced number of options. Because a limited range of options has been explored, bounded decision-making may lead to less than optimal results.

The absence of a well known and established WNVA framework could explain why most of the ten WNVA users would report that they endorse 'planning' in WNVAs but actually make little or no use of planning frameworks. The amount of time and expertise needed to find an appropriate framework, and then seek support for its use from senior management or other areas of the organisation, could discourage even those who claim to plan their WNVAs. The easier alternative would be to use no framework, and also carry out the WNVA without informing other organisational members. The time needed both to find and gain support for a procedure which other parts of the organisation are likely to misunderstand and mistrust, as well the fear of hacking mentioned earlier, could explain the finding that the majority of WNVAs users preferred that other organisational members not know that vulnerability assessments are used. As Takanen *et al.* (2004) have argued in their discussion of the distributions of responsibility among various actors in software vulnerability situations, this could compromise the ethical standards of the IT staff carrying out the procedure.

4 Conclusions

Organisational culture – especially because of its link with concerns in the wider society – may explain why IT professionals typically don't use either kind of WNVA or even seem to know about them. Wireless monitoring, as we have seen, entails surveillance of human activity on an important aspect of an organisation's infrastructure: its networks. On the one hand, as a population, we are becoming used to surveillance. We are being watched more than ever before, via cameras at shopping centres, e-tags in tunnels, and a vast range of electronic transactions. A lot of the time we are not bothered by this, and overlook how much surveillance is being done. An example of this 'aware and yet not aware' attitude is demonstrated in how a recent murder conviction in an Australian capital city was secured. The perpetrator claimed he was asleep at home in another city at the time of the crime, but evidence obtained from e-tag data – a form of daily surveillance that inner city drivers know about but forget – showed his car had been moving towards the victim's location shortly beforehand.

So we are often relaxed, 'knowing but unknowing', about surveillance. It is becoming part of our culture both in our organisations and outside them. However we are typically less sanguine when it is pointed out how much surveillance we are being subjected to. Australians have so far rejected smart identity cards, perhaps feeling that their convenience would be outweighed by increased surveillance they might lead to. Wireless monitoring, because it involves surveillance, could well create this ambivalence on the part of non IT staff. Even computer security staff may be ambivalent about wireless monitoring because of their concerns about how other organisational members will perceive them. Vulnerability assessments using penetration testing, with its overtones of an attack, could create even more anxiety. Again, while computer security staff may know that no real attack will happen, they may dislike being regarded by others as something akin to a hacker and having to explain their role. In short, employees, including IT staff, live in the external world as well as the world of their organisations. So while they are likely to see the need for computer security they may also be ambivalent about what they have to do to achieve it.

5 Recommendations

According to Dunphy and Stace (1993), dealing with the effects of organisational culture involves either living within the culture as it is and making the most of its positive aspects, or trying to change the culture.

5.1 Improving organisational security within the existing organisational culture

The implications for businesses wanting to improve their computer security are that they need to take account of how aspects of organisational culture may work against computer security as well as for it. With respect to wireless network security, they need to be aware of the anxieties – both internal and external – that are likely to be associated with WNVAs. Businesses have always needed to be mindful of how their activities are perceived by both their external and internal 'publics'. The difficulties of Enron, Shell, the Australian Wheat Board, James Hardie and many other firms which have been accused of poor behaviour, are due in part to what people – insiders as well as outsiders – believed they *could* do as well as what they actually *did* do. Living with this situation, as Spurling (1995) has shown, requires frequent and credible communication with the organisation's internal and external publics about why specific security strategies are necessary.

5.2 Improving organisational security by changing organisational culture

Tacit knowledge as embodied in organisational culture may be altered, although this is typically difficult and time-consuming. Various approaches to changing organisational culture in the interests of helping the organisation adapt to other necessary change have been examined by change theorists such as Argyris (1990), Dunphy and Dick (1981), Dunphy and Stace (1993), Kotter (1995) and Lewin (1951). These theorists all argue that specific changes should be embedded into the organisation's culture. Introducing a new security protocol would be an apt example of a change requiring this treatment. Embedding change into culture is typically the last and most difficult part of a planned change process, though often the most important if the change is to remain. A

major computer security breach or the threat of one may be sufficient to establish a sense of critical urgency needed to convince organisational members of the need to do things differently. This is the first step in most theorists' recommendations for successful planned change.

Embedding WNVAs into organisational culture could be helped by incorporating them, and an appropriate framework for carrying them out, into standard operating procedures. To apply Schein's ideas about the importance of organisational stories and rituals in transmitting and embedding aspects of culture, organisational stories about security breaches detected and harm avoided, preferably without damage to other employees' privacy and with appropriate rewards allocated, could over the long term change users' perceptions about the risks and rewards of WNVAs.

Such cultural change is unlikely to happen without problems. The necessary cultural shifts may well threaten aspects of ICT professionals' work identity, for example, since subcultures including those of IT professionals have been shown to depend in part on their special expertise which contributes to the power they can exercise in organisations (Jermier *et al.* 1991; Sackman 1992). This and other implications of the results of the present study, for example in the areas of IT professional ethics, computer security awareness education, and so on, requires further research.

References

Anonymous (2003) 'Wireless networks grow dramatically, but security remains a problem, report says', *Electronic Commerce News*, 8 (31 March).

Argyris, C. (1990) *Overcoming Organizational Defenses*. Boston: Allyn and Bacon.

Berghel, H. and Uecker J. (2004) 'Wireless Infidelity I: War Driving', *Communications of the ACM*, 47 (9), pp. 21-26.

Dunphy, D. and Dick, R. (1981) *Organizational Change by Choice*. Sydney, New York: McGraw-Hill.

Dunphy, D. and Stace, D. (1993) 'The Strategic Management of Corporate Change', *Human Relations*, 46 (8), pp. 905-20.

Dyce, K. (2005) *A Wireless Vulnerability Assessment Framework: A developed prototype wireless vulnerability assessment framework and a study into their use in the real world.* Unpublished Honours thesis, University of Wollongong.

Henning, R. R. (2003) *Vulnerability Assessment in Wireless Networks*, Harris Corporation, [Available Online: http://www.cs.nmt.edu/~cs553/paper15.pdf], Accessed 5 January 2006.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work Related Values*, Beverly Hills: Sage.

Hofstede, G. (1991) *Cultures and Organizations: Software of the Mind*, London: McGraw-Hill.

Hofstede, G. (1993) 'Cultural Constraints in Management Theories', *Academy of Management Executive*, (February), pp. 81-94.

Housley, R. and Arbaugh, W. (2003) 'Security Problems in 802.11-based Networks'*, Communications of the ACM*, 46 (5) (May), pp. 31-34.

Jermier, J. M., Slocum, J. W., Fry, L. W. and Gaines, J. (1991) 'Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Façade of an Official Culture', *Organizational Science*, (May), pp. 170-94.

Kotter, J. P. (1995) 'Leading Change: Why Transformational Efforts Fail', *Harvard Business Review*, 73 (March-April), pp. 59-67.

Lewin, K. (1951) *Field Theory in Social Science*. New York: Harper and Row.

O'Reilly III, C. A., Chatman, J. and Caldwell, D. F. (1991) 'People and Organizational Culture: A Profile Comparison Approach to Assessment of Person-Organization Fit', *Academy of Management Journal*, (September), pp. 487-516.

Nichols, R. K. and Lekkas, P. C. (2002) *Wireless Security: Models, Threats and Solutions*, New York: McGraw-Hill.

Peltier, T. R., Peltier, J. and Blackley, J. A. (2003) *Managing a Network Vulnerability Assessment*, Auerbach Publications, USA.

Sackmann, S. A. (1992) 'Culture and Subcultures: an Analysis of Organizational knowledge', *Administrative Science Quarterly*, (March), pp. 140-61.

Schein, E. H. (1985) *Organizational Culture and Leadership*. San

Francisco, CA: Jossey Bass.
Schein, E. H. (1993) 'On Dialogue, Culture, and Organizational Learning', *Organizational Dynamics*, (Winter), pp. 40-51.
Simon, Herbert A.. (1979) 'Rational Decision Making in Business Organizations', *American Economic Review*, 69 (4), pp. 493-513.
Spurling, P. (1995) 'Promoting security awareness and commitment', *Information Management & Computer Security*, 3 (2), pp. 20-26.
Takanen, A., Vuorijärvi, P., Laakso, M. and Röning, J. (2004) 'Agents of responsibility in software vulnerability processes', in *Ethics and Information Technology*, 6, pp. 93-110.
Tiller, J. S. (2005) *The Ethical Hack: A Framework for Business Value Penetration Testing*, Auerbach Publications, USA.

Author Biographies

Ms Roba Abbas is a final year honours student at the University of Wollongong, Australia. She is completing her Bachelor of Information and Communication Technology degree (majoring in Business Information Systems). Her research interests are focused on public data availability within the critical infrastructure space, in the context of regional Australia. Roba is also a part-time Solutions Analyst at Internetrix, Wollongong. ra75@uow.edu.au

Prof Mary Barrett is a Professor of Management in the School of Management and Marketing at the University of Wollongong, NSW, Australia. Her teaching interests are in the fields of human resource management, employment relations and general management. Currently her research focuses on gender issues in management, organizational communication, including its relationship with information security, and family business, including women in family business. She has published over 60 academic articles and 6 books. mbarrett@uow.edu.au

Ms Emilia Pérez Belleboni is a researcher in the VOTESCRIPT group at the Polytechnic University of Madrid (UPM), a lecturer in telecommunications engineering, and a PhD candidate in the Department of Engineering and Telematics Architecture. Emilia has presented her

work at international peer reviewed conferences in South America, including, “Architectural design for a digital democracy telematic platform” and “VOTESCRIPT: a telematic voting system designed to enable final count verification”. belleboni@diatel.upm.es

Mr Jesús Moreno Blázquez is a researcher in the VOTESCRIPT group at the Polytechnic University of Madrid (UPM), a lecturer in computer engineering, and a PhD candidate in the Department of Engineering and Telematics Architecture.

Prof Simon Bronitt is the Director of the National Europe Centre, Research School of Humanities and a Professor in the ANU College of Law. His research and teaching interests span criminal law and criminal justice, comparative law, with a special interest in covert policing, terrorism law and human rights. Recent publications include: *Principles of Criminal Law*, with B McSherry (2nd ed, Law Book Co, 2005) and *Law in Context*, with S Bottomley (3rd ed, Federation Press (2006). BronittS@law.anu.edu.au

Mr Mark Burdon graduated from South Bank University (now London South Bank University) with LLB(Hons) in 1996. He worked in the UK Civil Service at the Cabinet Office whilst studying his MSc(Econ) Public Policy at the University of London’s Queen Mary and Westfield College. He graduated in 1998 and his dissertation researched ICT implementation policies in central government. Following his studies, Mark worked at the Bloody Sunday Inquiry, the largest public inquiry in British history. The Inquiry developed a state-of-the-art hearing chamber using the most up to date courtroom technologies. He designed working processes involved with the new technologies and managed the Inquiry’s witness programme. Mark moved from the Inquiry and worked for the international law firm Freshfields Bruckhaus Deringer on the *Three Rivers* case, the largest piece of litigation in English legal history. Mark immigrated to Australia in late 2004 and started work with the Information Security Institute in September 2005. m.burdon@qut.edu.au

Prof 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. He has undertaken research, consultancy and public interest advocacy, and published extensively in Australia and overseas, in the areas of identification, security, dataveillance and social impacts and implications of information technology, for over 30 years. His website is one of the most extensive and most used resources in these areas. Roger.Clarke@xamax.com.au

Prof Peter Croll has been developing dependable software solutions for three decades in both industry and academia. He attained his PhD in 1990 from the University of Sheffield researching into safe designs of distributed real-time computer systems. He joined QUT in 2004 as their Professor of Software Engineering in the Faculty of Information Technology and as the Director of the research Centre for Information Technology Innovation (CITI). For three years previously, Prof Croll was Head of School for IT and Computer Science, at Wollongong University where he was also the Director of both their research institute for Telecommunications and IT (TITR) and their e-Health initiative. He is currently seconded as a Fellow of CSIRO's National Flagship on Preventative Health to investigate the privacy and security risks associated with electronic health data integration. Professor Croll is an active Fellow of the Australian and British Computer Societies, a Chartered Information Technology Professional and a Chartered Engineer. Prof Croll has attracted over $5 million in competitive funding and produced over 100 international research publications in refereed journals, conference proceedings and books. His research now focuses on risk-based development methods for producing high quality software for essential service industries. croll@qut.edu.au

Mr Keir Dyce recently completed a Bachelor of Information Technology at the University of Wollongong, achieving First class Honours. His supervisor was Professor Jennifer Seberry, Director of the Centre for Computer Security Research at the University of Wollongong. Keir is now working in information security for a major firm.

Mr Sergio Sánchez García is a researcher in the VOTESCRIPT group at the Polytechnic University of Madrid (UPM), a lecturer in telecommunications engineering, and a PhD candidate in the Department of Engineering and Telematics Architecture. Sergio has co-authored papers on the use of Java cards in telematic voting systems.

Prof Justo Carracedo Gallardo is a professor from the Polytechnic University of Madrid (UPM) and a senior member of the VOTESCRIPT research group having received his doctorate in computer science. Justo lectures in the Department of Engineering and Telematics Architecture.

Prof Margaret Jackson Professor of Computer Law and Director, Law Discipline in the School of Accounting and Law. Margaret is the author of *Hughes on Data Protection in Australia*, published by the LawBook Co in 2001, and *A Practical Guide to Protecting Confidential Business Information*, published by LawBook Co in 2003. Margaret is a member of the Smart Internet Technology Co-operative Research Centre and is involved in the Trust, Privacy, Identity and Security research stream. She is part of a research team exploring banking, personal communication and financial decision making and is also leading a research team exploring Identity Management and the Impact of Changing Roles in E-Commerce & M-Commerce. Recent articles have included: 'A Data Protection Framework for Technology Development', 'The Impact of DRMs on Personal Use Expectations and Fair Use Rights', 'Information Privacy Management by Digital Rights Management Systems', 'Black Hats and White Hats: Authorisation of Copyright Infringement in Australia and the United States' and 'Board Confidentiality'. margaret.jackson@rmit.edu.au

Mr Tim Lane is currently writing up his thesis as part of his QUT based

Masters by Research (IT). This study has 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

Mr Julian Ligertwood was admitted as a Barrister and Solicitor of the Supreme Court of South Australia in 2003. He has worked in legal research assisting academics and legal practitioners for more than seven years, most recently at Flinders University in Adelaide. Julian is currently a research fellow at RMIT University in Melbourne, working with Professor Margaret Jackson on issues of identity management. He is also completing a Masters Degree in Legal Theory. julian.ligertwood@rmit.edu.au

Ms Suzanne Lockhart is a criminologist with extensive practical and theoretical experience of the Australian criminal justice system spanning twenty years, specializing in biometrics and identity crime in mission critical public and private sector organizations. She has been a member of the Victoria Police and the Australian Federal Police. Suzanne's M.A Criminology degree at the University of Melbourne, researched the alignment between organizational requirements and community perspectives of biometric technology. She has specialized training in biometrics, criminal profiling and identity fraud and is currently engaged on an AUSTRAC sponsored Ph.D. researching identity fraud crime control policy at the University of South Australia. Suzanne has extensive knowledge of the biometrics industry both in Australia and overseas and has strong affiliations with international research institutions and close contacts with many Australian public and private sector organizations. She has delivered papers on identity fraud, biometrics, maritime crime and crime-terrorism convergence locally and internationally. Suzanne is one of three Australian representatives on the International Standards

Organization SC37 Working Group 6, Cross Jurisdictional and Societal Issues Committee, relating to the formulation of world wide biometric standards and is a member of the Australian Biometrics Institute Technical Committee. Suzanne consults with public and private sector organizations including the Department of Transport and Regional Services and the Department of Immigration and Multicultural Affairs. suzannelockhart@virtual.net.au

Prof Ana Gómez Olivia is a professor from the Polytechnic University of Madrid (UPM) and program leader of the VOTESCRIPT research group. VOTESCRIPT is a multidisciplinary research group focused on citizen participation telematic systems committed to the theory and practice of electronic voting and the digital democracy. It was established in the year 2000 and has thus far carried out a number of projects sponsored by the Spanish government in e-Democracy and e-Vote. Ana also lectures within the Department of Engineering and Telematics Architecture. She attained her PhD in Computer Science from UPM and has published widely.

Mr Carlos González Martínez is a researcher in the VOTESCRIPT group at the Polytechnic University of Madrid (UPM), a lecturer in computer engineering, and a PhD candidate in the Department of Engineering and Telematics Architecture.

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) in 2003, BIT (UTS) in 1996. She has worked in numerous industry positions including as an analyst for United Technologies in 1993 and Andersen Consulting in 1996, and a senior network and business planner for Nortel Networks (1996-2001). She is presently a senior lecturer at the University of Wollongong, Australia (2002-). In the School of Information Technology and Computer Science, Katina teaches eBusiness, strategy, innovation and communication security issues. Her current research interests are in the area of location-based services, geographic information systems and mobile solutions. She has written twenty-five refereed papers and is currently working on her first scholarly book titled *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. In her role with Nortel she had the opportunity to consult to telecommunication carriers throughout Asia, including Telstra, Optus, TCNZ, KGT, Bharti, Reliance, BayanTel, ONSE Telecom, China Telecom, SingTel, and HKTel. Dr Michael has been a member of the IEEE and ACM since 2005. katina@uow.edu.au ⅄ 61242213937 ⅄ http://www.itacs.uow.edu.au/school/staff/katina/

Dr M.G. Michael PhD, MA(Hons), MTh, BTh, BA is a theologian and historian with cross-disciplinary qualifications in the humanities. He has studied at Sydney University, the Aristotelean University (Greece), the Sydney College of Divinity, Macquarie University, and more recently the Australian Catholic University. Michael has been the recipient of a number of scholarships and awards. He is a member of the American Academy of Religion and an associate member of the *Association Internationale d' Études Patristiques.* Michael brings with him a unique perspective on Information Technology and Computer Science. His formal studies include Ancient History, Theology, Philosophy, Political Sociology, Ethics, and Government. He has authored papers in the disciplines of Biblical Studies, IT, and BioEthics. Presently the focus of his research extends to modern hermeneutics and the Apocalypse of John; the historical antecedents of modern cryptography; the auto-ID trajectory; and more broadly the system dynamics between technology and society. Michael has been a casual member of staff in the School of IT and Computer Science at the University of Wollongong since 2005. He is the

former co-ordinator and lecturer of Information & Communication Security Issues and has guest-lectured and tutored in IT & Citizen Rights, Principles of eBusiness, and IT & Innovation.

Dr Hasmukh Morarji is a Lecturer in the School of Software Engineering and Data Communications in the Faculty of Information Technology at the Queensland University of Technology in Brisbane, Australia. He has special interests in developing tools for teaching and learning Information Technology. He coordinated the project “Integrated Learning Environment for the Foundation Year of Bachelor of Information Technology” (ILE) under the Teaching and Learning Technology Grants Scheme. His current research interests include Computer Forensics where he is supervising a PhD student on the topic Computer Profiling for Forensic Purposes, applications of Software Engineering to large-scale systems, and e-Health. In e-Health his particular interests are (1) in an online web-based navigator to guide IT managers through the tools and techniques for evaluation and analysis of e-health information systems, and (2) to provide education and training to the users of IT in health. h.morarji@qut.edu.au

Ms Laura Perusco attended the University of Wollongong and graduated with a Bachelor of Information and Communications Technology with First Class Honours in 2005. Her Honours thesis focused on the social and ethical implications of the widespread use of humancentric location-based services applications. Laura has presented academic papers at conferences in Sydney and Beijing. Attending the 2005 *IEEE International Conference on e-Business Engineering* in Beijing was her first trip overseas. Laura currently works for Macquarie Bank, Australia’s market leader in the investment banking industry. laura_perusco@iinet.net.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. He is also Course Coordinator of the Doctor of Business Administration degree program. 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 has recently had articles on his research published in the *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*. Mark has for several years served on the Management Committee of the Illawarra Legal Centre, a community legal centre in the southern suburbs of Wollongong, and holds the position of Secretary and Public Officer. mrix@uow.edu.au

Prof Supriya Singh is Professor, Sociology of Communications and a Senior Research Fellow with RMIT Business, Royal Melbourne Institute of Technology University. She is a project leader with the Smart Internet Technology Cooperative Research Centre and a participant of the Research Network for a Secure Australia. Supriya's research interests cover the domestic aspects of globalization, user-centred design of information and communication technologies, sociology of money and banking, and qualitative research methodology. She combines these perspectives in her current study of security, trust, identity and privacy in banking within the social and cultural context. Her books include *Bank Negara Malaysia: The First 25 Years, 1959-1984* (Bank Negara Malaysia: 1984), *On the Sulu Sea* (Angsana Publications, 1984), *The Bankers*

(Allen and Unwin: 1991) and *Marriage Money: The Social Shaping of Money in Marriage and Banking* (Allen & Unwin, 1997).

Mr James Stellios is a Senior Lecturer at the ANU College of Law. Prior to joining the faculty at the ANU in 2001, he spent a number of years in legal practice working for the Commonwealth Attorney-General's Department and the Australian Government Solicitor, principally in the area of constitutional litigation. Immediately prior to joining the ANU College of Law, he was Counsel Assisting the Solicitor-General of the Commonwealth, and appeared as junior counsel for the Commonwealth in a number of constitutional cases before the High Court of Australia. He has also worked as a senior legal officer at the High Court. James is also a Consultant to Clayton Utz Lawyers, specialising in providing advice to the Commonwealth on public law issues. He holds a Master of Laws from Cornell University specialising in international and constitutional law, and has published widely in those fields. With Professor Simon Bronitt, has recently published "Telecommunications Interception in Australia: Recent Trends & Regulatory Prospects" (2005) 29 *Telecommunications Policy* 875. StelliosJ@law.anu.edu.au

Ms Holly Tootell is a Lecturer in the School of Information Technology and Computer Science 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. Holly is the Secretary of the newly formed Australian chapter of the IEEE Society on Social Implications of Technology (SSIT). Holly will be presenting her research at the International Symposium on Technology and Society (ISTAS) in New York in June. holly@uow.edu.au

Mr Adam Trevarthen completed his Bachelor of Information and Communication Technology (BICT) degree with First Class Honours from the University of Wollongong in 2005. He was awarded the University Medal for the highest weighted average mark. His honours thesis titled: "the importance of utilising electronic identification for total farm management" focused on the adoption of RFID technology by dairy farms

on the South Coast of NSW. Adam now works for Pillar Administration in Wollongong as a systems analyst.

Mr Jose David Carracedo Verde is a sociologist from the Complutense University of Madrid (UCM). He is a member of the VOTESCRIPT research group and is currently completing his PhD. Jose is focused on researching telematics and sociology, and has written papers on the importance of maintaining citizen privacy in electronic transactions (e.g. using credit cards).

Dr Marcus Wigan 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. He 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 has long been active with the Australian Privacy Foundation, particularly 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 work in Scotland is 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