2007

Auto-ID and location-based services in national security: Social implications

Holly Tootell
University of Wollongong, holly@uow.edu.au

Auto-ID and location-based services in national security: Social implications

Abstract

This paper provides an overview of auto-ID and location-based service technologies that are currently being used for the purposes of national security. The paper addresses the social dimensions of technology which have a bearing on their acceptance by individuals. This overview from both a technology and social perspective allows for an understanding to be created as increasingly decisions regarding adoption need to be made by different sectors in society.

Disciplines

Physical Sciences and Mathematics

Publication Details

Tootell, H. (2007). Auto-ID and location-based services in national security: Social implications. In K. Michael & M. G. Michael (Eds.), From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society (pp. 201-224). Wollongong: University of Wollongong.

15

Auto-ID and location-based services in national security: Social implications

Holly Tootell

Lecturer, School of Information Systems and Technology, University of Wollongong

Abstract

This paper provides an overview of auto-ID and location-based service technologies that are currently being used for the purposes of national security. The paper addresses the social dimensions of technology which have a bearing on their acceptance by individuals. This overview from both a technology and social perspective allows for an understanding to be created as increasingly decisions regarding adoption need to be made by different sectors in society.

Keywords: automatic identification, location-based services, national security, terrorism, liberty, privacy, security

1 Introduction

The primary purpose of a literature review is to provide evidence of relevant research being conducted in a particular field of study. This paper explores the use of auto-ID and location-based services technologies for national security purposes. This includes discussion of technologies currently being used, and also discussion of technologies being proposed for national security applications. Firstly the development and role of location technologies is covered in regard to national security. Secondly, a critical review of the social constructs that relate to the introduction of the technologies is necessary. This issue is addressed through the social dimensions of the technology, sometimes thought to be the consequences of its use: privacy and security. These concepts need to be treated separately but are closely related. Thirdly, the current context of national security and technology will be examined.

2 Background to automatic identification and location-based services

The following sections provide a review of auto-ID and LBS technologies. Each section begins with an overview of the technology and then moves to examine their presence in the national security arena. The sections have been organised in line with the historical development of the technology. This progression reflects an increase in precision of location identification.

Auto-ID technologies are those capable of providing automatic identification where human intervention is not required (Ames 1990a, b, c; Cohen 1994; Michael et al. 2006b). Auto-ID has traditionally been equivalent with barcodes, used on goods in stores and cards for financial transactions. The scope of use is now more widespread, with uses ranging from immigration control systems to pet identification. Auto-ID technologies have had a mass market presence since the 1960s and their potential for detrimental impact on human rights and privacy have been noted since the 1970s (Michael and Michael 2004, p.434).

The following technologies have been developed over the past 50 years. The drivers for this technology development have been the move by governments to adopt electronic systems to replace the use of paper-based methods (such as vouchers, coupons, ration cards and concession cards) to operate large-scale federal and state programs, in order to increase efficiency (Michael and Michael 2006a, p.21). Other reasons include greater social acceptance and affordability of the technology. Each of the following technologies has made a significant contribution to the area of location-based services, however it is their convergence that is of interest as discussion moves toward the role of location-based technologies in relation to national security. Smart cards, biometrics, RFID, GPS and GIS are technologies that alone or in combination provide information about the location of a user. Biometric technologies do not track location directly, but biometric identification

on a smart card ensures that every time the smart card is used to access a building for example, a time and date stamp of that biometric identification and smart card access is logged. This is able to be pieced together to enable movement patterns to be established. GPS on the other hand is a real-time location tracker.

This research is concerned with the issue of the automatic identification of people through location determination for national security purposes, in order to understand whether a trade-off is made for enhanced perception of security, or sacrificed in order to maintain an illusion of security.

2.1 Smart cards

A smart card is a credit card-sized plastic card that consists of an integrated circuit or 'chip' which enables the card the ability to store and/or process data. There are two broad categories of smart cards: memory cards that contain only non-volatile memory storage components, and perhaps some specific security logic; and microprocessor cards that contain memory and microprocessor components.

Smart cards emerged from the development of magnetic strip cards. The innovation of the smart card was devised by Juergen Dethloff of Germany. The first patent, although restricted to Japan, was taken out by Arimura in 1970. The first international patent was given to Frenchman Roland Moreno in 1974, who founded the Societé Internationale pour l'Innovation. This society was established to develop new technologies and extend its patents world wide (Rankl and Effing 2000; Zoreda and Oton 1994).

Smart cards have been adopted by many industry sectors for a variety of purposes. Table 1 provides an overview of some of the most common applications (Chaum 2000). In addition to these examples, smart cards are commonly used as access cards to secure areas, as identification cards and as loyalty cards for many different sectors.

Table 1: Smart Card Applications

Industry	**Application**
Financial	Electronic Purse, Credit/Debit cards and Secure Electronic payments
Transport	Electronic Toll collection, public transport fares and Drivers Licence
Communication	Mobile Phone accounts and Access to Pay TV
Healthcare	Medical Information cards and Government health insurance eligibility
Education	Identification, library access, security access
Government	Non-repudiation device for voting and Government benefit payments National Identification schemes
Retail	Discount/VIP/membership cards

The technological development of smart cards has advanced the cards to include larger memory and processing capacity which has increased the functional potential for their application. In line with this is a perceived increase in the threat posed by multi-purpose smart cards in terms of centralisation of data storage. This concern is

addressed specifically in regard to smart card national identification schemes by:

> …the simple logic that the higher an ID cards value, the more it will be used. The more an ID card is used, the greater the value placed on it, and consequently, the higher is its value to criminal elements (LSE 2005, p.35).

2.2 Biometrics

Biometrics, as a form of identification, have been in use since early fourteenth century China (Chirillo and Scott 2003, p.2). The earliest recorded uses of biometric identification include Babylonian kings who used handprints to identify different things such as engravings as their own (Harris and Yen 2002); and Chinese merchants in the fourteenth century stamping children's palm prints and footprints on paper with ink to be able to distinguish between them (Chirillo and Scott 2003).

A biometric is a "measurable physiological and/or behavioural trait that can be captured and subsequently compared with another instance at the time of verification" (Ashbourn 1994). It refers to identifying a person based on his or her distinguishing physiological and/or behavioural characteristics (Jain et al. 2000). Biometric identifiers include digital fingerprints, retinal scans, hand geometry, facial characteristics, and vocal patterns.

The public perception of a biometric identification technology is an important component in the success and adoption of a technique. In addition to this, the technique must be legally and physically robust, safe to use, and not invade the user's privacy. An example of this is a fingerprint scanner, which is often associated with criminal identification. The self-protection reflex of the eyes means that many people are uncomfortable with having laser scans on a regular basis and are often fearful of unfounded claims that regular scanning could be detrimental to their health. To contrast this, hand geometry scanning and signature verification are mostly regarded as innocuous (Kim 1995). One of the mistakes often made in the discussions of biometrics and use of parts of the body for identification is where the act of identification can be associated with a violation of bodily integrity (van der Ploeg 1999). Overcoming public perception of the invasiveness of the scan or acquisition of the biometric sample is the key to success of more pervasive use of these technologies.

From the perspective of civil libertarians, biometric identification has been seen as a threat to the location privacy of individuals (Davies 1998; Johnson 2004). However the counter argument recognises that many of the biometric identifiers being requested of a person are things that they have on show most of the time. There is nothing private about your face (Branscomb 1994; Scheeres 2005). The same was said of voice and handwriting by the US Supreme Court. A person's reasonable expectation of privacy could not extend to "those physical characteristics that are constantly exposed to the public" (Woodward Jr 1997, 2001). However, this does not overcome the controversy related to the legal issues surrounding the storage

and usage of biometric identification (Chandra and Calderon 2005; van der Ploeg 1999).

Biometric identification can be used for many purposes. Table 2 groups the uses into three broad categories; forensic, civilian and commercial, and describes typical uses for these forms of identification (Jain et al. 2000; Petersen 2001; Rood and Hornak 2003).

Table 2: Applications for Biometric Identification

Forensic	Civilian	Commercial
Criminal investigation	National ID	ATM security
Corpse identification	Driver's license	Credit card security
Parenthood determination	Welfare disbursement	Cellular phone
Prison security	Border crossing	Access control
	Customs and immigration initiatives	Ecommerce/ebanking transactions
	Protecting critical infrastructure	

Biometric identification is extremely useful for restricting access to areas that involve national security, such as military bases or intelligence centres, and for protecting critical civilian infrastructure, such as water supplies and power plants (Rood and Hornak 2003). It must be noted that technology such as this is not a panacea. No technology solution is absolutely foolproof (Michael and Michael 2006b, p.360).

Some biometric identification programs are mandatory, for example criminal investigation and prison security. At present, almost all other programs are voluntary. However, in some of the programs, biometric identification is used to make the service more attractive to users by providing a faster, or more enhanced service, but other forms of identification are still permitted (Alterman 2003). An example of this is the INSPASS (Immigration and Nationalization Service Passenger Accelerated Service System) program in the US. It has been operating since August 1993 as a voluntary system for frequent travellers. It allows passengers to move through immigration more quickly at the cost of a system that has the potential to create a vast amount of international transfer of their personal data (Davies 1996; Kim 1995). This system has grown from 2000 frequent fliers at the outset, to over 100 000 by the year 2000 (Michael and Michael 2006a).

Van der Ploeg (1999) considers the groups targeted for obligatory biometric identification disproportionately include criminals, recipients of welfare, or other benefits, workers, and immigrants. However she classifies an alternate grouping where biometric identification may typify privilege as well. It may include frequent flyers who have been assessed as 'low-risk travellers', are given the privilege to jump the queue and avoid thorough controls; those who have higher access privileges to

secured spaces, parts of IT systems or authorisation of high-risk types of financial transactions.

Biometrics have the potential to enhance our current reliance on documents such as birth certificates, drivers' licences, and passports to establish each person's true identity. In the future, biometric information may be recorded at birth and incorporated in the birth certificate, using the child's DNA as the prime indicator of identity. In such a case, a person's biometric information (which may change with age) may be linked with his DNA (Rood and Hornak 2003).

2.3 Radio frequency identification

Radio Frequency Identification is a technology used for automatic identification. RFID is a generic term for technologies that use radio waves to automatically identify entities; either live or inanimate. The objects are identified by information that may include a unique identifier, or it could be more complex including data such as: manufacturing history, temperature, or age (Kinsella 2003; Legner and Thiesse 2006).

RFID has been referred to as the new barcode (Kelly and Erickson 2005; Want 2004). The advent of barcode technology revolutionised data capture and handling technologies in the retail industry. RFID has advanced data capture and stock handling to a new level. One of the main advantages of RFID is overcoming the reliance of barcodes on line-of-sight data processing. RFID offers more robust and useful scanning options (Alippi and Vanini 2004; Srivastava 2007). Other advantages discussed by Michael et al. (2006b) are that RFID is not limited by its size and is not vulnerable to magnetic fields, or affected by substances such as dirt or paint which may cover the tag.

RFID systems are being used for many item-level tracking applications. The phrase 'internet of things' is being used to describe the potential network of information that could be created by the use of RFID in the following applications (see Table 3) (Alippi and Vanini 2004; Elliot 2003; Floerkemeier and Lampe 2004; Garfinkel et al. 2005; Hsi and Fait 2005; IIE Solutions 2002; Jayakumar and Senthilkumar 2005; Jones et al. 2004; Juels 2006; Smith 2005; Swartz 2004; Want 2004).

Since September 11 the threat of terrorism has ensured that the tracking offered by RFID is a favoured system implemented to alleviate that threat, be it in shipping containers or passport control. Atkinson (2004) observed that prior to September 11 the use of RFID was limited to supply chain security and loss prevention, however in the post-September 11 world, the focus for RFID is ensuring tamper-proof containers due to terrorism concerns. The continued development of RFID technologies is regarded by many to have a significant impact on the way we conduct our day to day life. US Senator Patrick J. Leahy stated that:

> RFID has tremendous potential for improving productivity and security, but it will also become one of the touchstone privacy issues of our times (Swartz 2004).

Table 3: Commercial RFID Applications

Application	Commercial Examples
Baggage tracking in airports	For airport baggage identification, RFID has eliminated the need for manual sorting and lifting and is claimed to have enhanced passenger security.
Supply chain management and supply chain theft reduction	The clothing giant, Prada, have their New York dressing rooms fitted with display screens that can identify a smart-tagged garment when it is bought into the room. The display suggests other styles and colours of the garment - even going so far as to show how the garment was worn at a Prada fashion show.
Automobiles	Remote keyless entry.
Animal tracking	Identification and tracking for enhanced livestock management
Highway toll collection	Highway toll collection using RFID has allowed drivers the convenience of driving straight through checkpoints without needing small change.
Passport security	The inclusion of RFID tags in passports and possibly drivers' licenses acts as an 'anti-counterfeiting feature.
Museum exhibits	Enhancing interactivity of displays.
Automatic product tamper detection	Product integrity can be monitored from factory to retail location. It might also help locate the source of activity when tampering is detected.
Harmful agent detection	The use of passive-detector technology could be used on vehicles or security personnel, or in other uses where detection of biological agents are needed.

This sentiment was reflected by Rick Duris, from frontline Solutions Magazine, and recorded by Albrecht and McIntyre (Albrecht and McIntyre 2005):

> RFID will have a pervasive impact on every aspect of civilization, much the same way the printing press, the industrial revolution and the Internet and personal computers have transformed society…RFID is a big deal. Its impact will be pervasive, personal and profound. It will be the biggest deal since Edison gave us the light bulb.

The pervasiveness in Duris' observation is seconded by Borriello (2005, p.36) who believes that there is an imaginable future where; "Passive RFID tags are in every manufactured object and maybe even in some non-manufactured ones (such as natural resources, animals, and people)."

The US Department of Homeland Security is now using RFID technology at US border checkpoints (Swartz 2004). Visitors entering the US will be issued RFID tags that will track their comings and goings at border crossings. The technology was tested at border crossings in Arizona, New York, and Washington state from the end of July through to spring 2006 (Chabrow 2005). Angell and Kietzmann (2006) puts forward the hypothetical of RFID cash being the preferred method of transaction in the post-September 11 environment, where the threat of anonymity could be removed.

In emergency response situations, like the 2004 Boxing Day Tsunami and 2005 Hurricane Katrina, RFID tags can, and did, assist in management and location

identification of survivors as they were moved between emergency housing facilities or graves (Smith 2005).

Consumer response to RFID is a considerable factor in the future of the technology. Consumer perception is often linked to perceived risks relating to personal data privacy, tracking and remote scanning (Hsi and Fait 2005, p.65; Nath et al. 2006, p.24). Eckfeldt (2005, p.78) puts forward that a clear value proposition to customers is what distinguishes between a successful and shunned RFID application. This is seconded by Ohkubo et al. (2005, p.68), who also raises the problem associated with killing an RFID tag as a privacy protection measure. He suggests that if the tag was 'killed', the consumer would not be able to take advantage of "future emerging services that would rely on the millions of RFID tags likely to be dispersed throughout the consumer environment". A survey by Metro Group, investigating consumer's major privacy fears relating to RFID found that:

> Regardless of privacy-enhancing technology employed, consumers feel helpless toward the RFID environment, viewing the network as ultimately more powerful than they can ever be (Gunther and Spiekermann 2005, p.74).

2.4 The global positioning system

The Global Positioning System (GPS) is a satellite-based navigation system. It is used by both military and civilian users. GPS allows for precise location determination however accuracy is different for civilian and military applications. The location is determined based on the distance a user is away from the available satellites. The effectiveness and accuracy of GPS can be affected by weather conditions, mountains, buildings and other terrain (El-Rabbany 2002, p.1; Michael and Masters 2006; Oderwald and Boucher 1997, p.2). The most significant drawbacks of the technology for civilian applications are regarded as low availability/coverage in high-rise urban settings, no system integrity and no guarantee of services performance in a shared military/civilian environment (The Royal Academy of Engineering 2004). Getting (1993) believes GPS to be "…the most significant development for safe and efficient navigation and surveillance of air and spacecraft since the introduction of radio navigation 50 years ago".

GPS has been used for over two decades. In that time the range of uses has expanded enormously as the cost of receivers has become less. Areas of applications are outlined in Table 4 (El-Rabbany 2002, p.129-150; ESRI 2007).

Designed primarily as a military tool, GPS is used to facilitate accurate location awareness. This can be applied to command and control of forces and targeting of weapons. Geographical Information Systems (GIS) are systems used to create and manage spatial information. GPS has the ability to identify events that happen in large, hard to monitor areas like borders, harbours or military bases (Friedrick 2003). For security agencies, there is the ability to more accurately manage resources and access privileges once an incident has been identified.

Table 4: Commercial Applications of GPS

Application	Commercial Example
Mapping	Asset management for utility companies and airborne topographic mapping.
Resource Management	Forestry and natural resources: fire prevention, harvesting, aerial spraying.
Farming	Harvest yield monitoring, chemical applications control and property management.
Civil Engineering	Road construction, earth moving and equipment tracking.
Mining	Assistance with drilling, vehicle tracking and surveying.
Surveying	For both land and marine seismic surveying.
Navigation	In-vehicle street directory systems.
Transit	Mass transport: position determination, fleet management and timetabling.
Retail	Delivery fleet monitoring and dispatch assistance.

3 Social dimensions of technology

With regard to technology, security and privacy are often used interchangeably. To ensure privacy of information, security is required; and vice versa, without privacy safeguards in place, security could be compromised. The following sections detail the concepts of privacy and security as they can be experienced by individuals. Other related concepts including surveillance and liberty are also addressed. These concepts are relevant to discussions of the information society, and the power that exists within that framework, which are addressed in the final section. The importance of addressing these aspects in relation to technology is discussed at length by Ellul (1965, p.90), who reminds us that the consequences of a technology are not necessarily of technical significance, but can be of social or organisational consequence.

3.1 Privacy

Privacy is a concept that has eluded a single, clear definition. McLean (1995) likens privacy to the concepts of liberty and freedom: each a concept unable to be easily defined. To define privacy is to limit its scope (Day 1985; Schoeman 1992). Many cultures do not have a single word for the concept the English language knows as 'private' or 'privacy'; this reflects on the complexity of the concept. Day (1985) dedicated an entire thesis to the definition of privacy across cultures and languages and found some five hundred definitions. However, for the purposes of this work, a working understanding is necessary.

Privacy has been recognised as a concept that has evolved with the progress of society, changing to suit the demands of the current times (Gotleib and Borodin 1973; Rule et al. 1980). Warren and Brandeis (1890) first wrote of the right of privacy in 1890, asserting that privacy was the right to be left alone. Clarke (1997) prefers not to assume privacy is a right: as a right implies an intrinsic and absolute standard,

something not always applicable to privacy. Recognising privacy as an interest that an individual sustains allows for a more flexible definition that suits the application of privacy in both the offline and online environment: a description suited to the purposes of this work.

Privacy and surveillance, although being distinctly separate concepts, continue to be linked together through popular media including fiction and films. This reinforces a perceived public concept of them being one in the same. Popular movies that show this include: Rear Window (Hitchcock 1954), Blowup (Antonioni 1966), The Conversation (Coppola 1974), The Osterman Weekend (Peckinpah 1983), Sneakers (Robinson 1992), Lost Highway (Lynch 1997), Gattaca (Niccol 1997), The End of Violence (Wenders 1997), Enemy of the State (Scott 1998), The Truman Show (Weir 1998), Antitrust (Howitt 2001), Panic Room (Fincher 2002), Minority Report (Spielberg 2002), Collateral (Mann 2004), Cache (Haneke 2005), The Good Shepherd (De Niro 2006), The Departed (Scorsese 2006) and Déjà vu (Washington 2006). In the literary world, George Orwell's Nineteen Eighty Four (1949) is an archetypical expression of what life would be like in a totalitarian state where privacy did not exist.

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment (Orwell 1949).

3.2 Surveillance

Surveillance has been considered to be an important concept over a long period of time; it derives from the French Revolution at the end of the 18th Century. Wigan and Clarke (2006) define three functions for surveillance when it is utilised as a security safeguard: "to anticipate a violation... to detect a violation... or to assist in the identification of the person responsible for a violation or in the authentication of an assertion as to the identity of the culprit".

In the recent past surveillance has risen to a higher level of interest. This can be attributed to the increase in database systems collecting information about us (Garfinkel 2000) or it can be likened to the concepts of 'dataveillance' or 'panoptic sort' described by Clarke (1997) and Gandy (1993) accordingly. Both of these terms relate to the ability of collections of information to be equated with power. The increase in technological capability over the past few decades has seen an increase in the potential of machines and systems to collect information and then data mine. The transition to an online economy, or at the very least, online commerce, has created a whole new pool of information to be collected, tracked and stored. Clarke (1997) and Gandy (1993) recognised that collection of data was occurring well before the online world came into existence.

The introduction of online communications, and more particularly electronic commerce, has resulted in a changing attitude to control of privacy. Privacy in the online environment can be considered differently to a 'traditional' notion of privacy. Privacy in the online arena is mostly concerned with the protection of information. The term 'information privacy' has been defined by Clarke (1997) to be an interest held by individuals regarding the control, and handling of data about themselves. Gandy (1993) supports this theme in his notion of 'informational privacy' based on Westin's (Westin 1967) work as the "claim of individuals… to determine for themselves... the extent information about them is communicated to others".

3.3 Data surveillance

Data surveillance, or dataveillance as defined by Clarke (1988), is the:

> …systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.

It describes the surveillance practices facilitated by the collection and storage of extensive quantities of personal data. The notion of data surveillance is supported by Flaherty (1989) who classifies the practice of data surveillance within the broader notion of surveillance as the "supervision, observation or oversight of individuals behaviour through the use of personal data" (Davies 1996, p.248). The use of the term data surveillance is quite narrow, however it is very similar to a number of more specific terms outlined below: Langford (2000, p.73) has likened the concept of data surveillance to the practices of data matching, data monitoring and data recording. Bennett (1996) describes the concept of data surveillance as computer matching.

Lyon (2002, p.353) attributes the pervasiveness of data surveillance to the resulting convergence of information technology structures, the Internet and the vast amounts of data which both are able to provide. Barr (1994) believes that the concept of the information society has contributed to the increase in potential of data surveillance. Clarke (1988) believes that the application of information technology has been a factor in the increasing trend towards surveillance technologies and their pervasive use in the surveillance of individuals through the use of personal data. In contrast to these theories based on data surveillance being an entirely new concept, Langford (2000, p.74) believes that the Internet is inextricably linked to and is responsible for the exacerbation of data surveillance techniques and suggests that it has not facilitated, but merely enhanced previously existing techniques.

As Langford (2000) suggests, the concept of surveillance techniques, such as dataveillance, cannot only be attributed to the Internet and other information technology trends, as much contemporary literature tends to suggest. This form of surveillance has been used extensively within paper-based and localised data systems. Subsequently, the Internet and similar trends have not created this new form of surveillance, but merely facilitated the growth of such by utilising existing

techniques by providing access to more information and technology for exploitation (Lyon 2002, p.346). This has been recognised by the Office of the Federal Privacy Commissioner in understanding that the internet has only contributed to the "proliferation of uses of personal information" (OFPC 2006) rather than initiating such dataveillance practices. An extension to the concept of dataveillance has been proposed by M.G. Michael (Michael et al. 2006a): überveillance. This term describes a level of surveillance that goes beyond the scope of 24/7 surveillance. M.G. Michael presents the issues for concern as "misinformation, misinterpretation, and information manipulation."

3.4 Security

Security can be used to describe many different issues but in the context of this research it is about protection (Acharya 2002). The relationship between security and privacy is often blurred, Starner (2001, p.57) distinguishes between them in the following excerpt:

> Security involves the protection of information from unauthorized users; privacy is the individual's right to control the collection and use of personal information.

This is particularly of interest in the context of national security technology innovations such as national ID and terrorism prevention measures (Michael and Michael 2004). Security as a personal pursuit is being free from threat to personal safety. The security in this instance is a perception or 'feeling' experienced by an individual which means it is likely to be experienced differently for each person. In terms of the preceding sections and Starner's (2001) definition given above, security needs to be considered as technology systems that create information are developed. In relation to the auto-ID and location-based technologies focused on in this work, the potential for privacy invasion to occur is high, which is why the need to be aware of security implications is necessary.

A recurrent theme in technology implication discussions is the prospect of a trade-off between privacy and security. Snow (2004, p.156) defines security as a variable dependent on two issues: factors that threaten the things we value and our interpretation of the environment. In this definition, it is clear that security, if placed on a continuum, could have infinite variation depending on personal interpretations of these factors.

4 National security and technology

4.1 National or homeland security

The specific notion of security in relation to protecting a country from threat has been known variously as homeland security and national security. The concept has been linked closely with military developments at points in time, and at others, has referred to a much broader spectrum of protective initiatives designed to

ensure peace is maintained and the stability of government and society. 'Homeland security' has been predominantly found in US-based literature following the events of 11 September 2001. Since then the term has been gaining wider global acceptance. National security is often used interchangeably with homeland security, internal security, border management and counter terrorism (Relyea 2002). In the literature, homeland security is often linked to terrorism. This limits the scope of the discussion, which enables the introduction of the term national security to be a more encompassing phrase to describe the current state of affairs. For the purposes of this thesis national security encompasses the following categorisations as defined by Kun (2004): intelligence gathering and warning; border and transportation security; domestic counter-terrorism; protection of critical infrastructure; defending against outside attacks; and emergency preparedness and response.

The rhetoric since September 11 has focused on the idea of the homeland and the need for it to be protected and kept free from attack. The language of government and media coverage has encouraged the development of the theme of war on terror. This creates bias in the coverage of homeland awareness.

4.2 Sweeping changes in the name of national security

The recent focus on national security has renewed interest in technologies with the potential to be used for security measures. A technology that has experienced this refreshed approach is biometric imaging. Prior to September 11, it was discussed in primarily defensive terms, as public interest focused on the more sinister potential of the technology, and not the improved security potential it could offer. In the immediate period following the attacks, airports announced urgent implementation of scanning programs, and governments undertook expedited reviews of biometrics-based security systems.

The Defense Advanced Research Projects Agency has initiated a project called Human ID at a Distance which aims to "develop biometric technologies… that can be deployed to identify a known terrorist before he closes on his target" (Alterman 2003). The US Department of Defense (DoD) is supporting research into the application of biometrics, establishing the Biometrics Fusion Centre in Bridgeport, West Virginia. The centre is to help evaluate, implement, and integrate biometric technologies for DoD organisations. The US DoD has adopted a smart card (with an embedded chip) as the standard method of identifying its employees and controlling access to its sites. The DoD plans to add biometric information to the card within the next year (Alterman 2003).

The ability of biometric systems to grant authorised users access to privileged information and protected devices, while denying the same access to others, means that they can assist with the protection of military facilities, airports, industrial plants, offices, retail stores, personal residences, and recreational areas. Rood and Hornak (2003) have questioned whether this form of identification and management of person access would have prevented the events of September 11.

4.3 Legislative changes

The events of September 11 were a turning point for legislative changes. Although the US, UK and Australia had counter terror measures in place, many changes were made in the period since September 11 (Goldstone 2005; Northouse 2006). Some of the changes have met with much criticism from civil rights groups as they are seen to stretch the limits of allowable actions.

The United States Congress passed the following Acts which enhanced the reach of biometric identification of citizens and aliens: the PATRIOT Act – several measures to improve the government's ability to detect foreign threats operating in the United States. Wire taps surveillance and subpoenas; the Aviation and Transport Security Act and Enhanced Border Security and Visa Entry Reform Act

These were privy to an extraordinarily fast track through to becoming legislation which was noted by many civil libertarians. This fast track came in the presence of warnings prior to September 11 that the US Department of Defense did not have concrete plans in place to address emerging threats (Michael and Masters 2006).

The change in this approach has had follow-on effects to other countries. Australia and UK have border control law updates, and more dangerously, it is being used as a ruse to justify other far greater repressive actions (Goldstone 2005, p.165). The technology impact can be seen in the biometric passport system implemented in Indonesia, considered to be the world's most comprehensive and decentralised (Poessl 2006); the implementation of BioPass in Singapore, which claims to have enhanced security features to prevent tampering (Yeo 2006) and, Thailand has started issuing citizens with a Java-based multi-application smart card, used primarily for security purposes in the initial deployment (Bergman 2005).

5 Social implications of national security

5.1 Liberty

Liberty, as defined in the Oxford Dictionary of Philosophy, is of concern in almost all constitutions. It associates the value of liberty with autonomy, and as dependent upon the nature of the social context rather than on individual rights ("liberty" 1996). Liberty is also understood as

> …the right or power to do as one pleases …right, power, opportunity, permission …freedom from control by fate or necessity …a right, privilege, or immunity, enjoyed by prescription or grant …setting aside of rules or convention ("liberty n." 2004).

It is this list of expected freedoms that some fear is being threatened in the post-September 11 world. Increasing technology pervasiveness is a threat to being free, or doing as one pleases. At extremes, it is taking away the power of choice. The adoption of auto-ID and location-based technologies in a mandatory scheme will challenge this definition of liberty. There is certainly a need to balance effective law

enforcement initiatives in the threat of terrorism, but commentators are pleading for it to be done with respect for civil liberties (Goldstone 2005; Luban 2005; Northouse 2006).

Liberty is inextricably bound together with the human rights movement which is bringing privacy and security issues to the fore. From the research examined, the concept of liberty encompasses the notion of civil liberties. Civil liberties, although an essential part of our society, are often taken for granted where there is no direct threat. Goldstone (2005, p.159) suggests that when society is free of security threats, civil liberties are rarely in danger, but in times of war there is a real danger of overreacting. His comments are particular to the United States in this work, but hold true in a wider realm. Luban continues this theme, distinguishing between times of danger and peace. He draws the concepts of security and liberty together through an inevitable trade-off.

> …and the only important question then becomes where to draw the line. How much liberty should be sacrificed in the name of security (Luban 2005, p.242).

5.2 Paying a price

Throughout the research on existing studies, there is a consistent theme of citizens needing to waive certain liberties or have reduced access to services in order for national security initiatives to be fully implemented. This is particularly noticeable in the privacy-based studies. The concept of this can be summarised as the figurative price that the average citizen is 'paying' for this increased level of national security.

However, the concept goes back much earlier and in consideration of many more issues than the rapid advancement of technologies. Over time, identifying the price that is being paid for advancement is a difficult task, and it is harder still to measure. Winner frames this observation in terms of consumer product developments and makes the comment that:

> They have gotten used to having the benefits of technological conveniences without expecting to pay the costs. Of course, if anyone had bothered to notice, it should have been obvious that a price for "progress" was being paid all along. It was often a very subtle price, a barely recognizable price, but a real one nevertheless (Winner 1986, p.171).

In Winner's research it is suggested that when people want something to happen, they will find ways to justify the costs that need to be paid. It seems inevitable in this model that it is only when the changes occurring through the payment of costs have gone too far that people are able to step back to look objectively at the impact those decisions have had on their life. The pervasive impact of technologies on daily life is questioned only when certain boundaries are challenged. Winner (1986, p.50) proposes the following issues as costs that are significant enough to

consider limiting the use or development of a technology:

- Its application threatens public health or safety;
- Its use threatens to exhaust some vital resource;
- It degrades the quality of the environment (air, land, and water);
- It threatens natural species and wilderness areas that ought to be preserved;
- Its application causes social stresses and strains of an exaggerated kind.

Ng-Kruelle et al. (2002) established the concept of 'Price of Convenience' as a means for understanding what a consumer is willing to give up of their privacy in order to gain a factor of convenience. This study examined the use of mobile devices. This research has established a direction in technology studies to look beyond the benefits of the tool itself and instead evaluate the impact it can have on the end user. Ng-Kruelle et al. (2002, p.4) discuss the concept of the "price" in the context of mobile commerce applications and the consumer. The phrase under consideration here is the 'Price of Convenience':

> At an individual level, any potential "consumer" must always balance costs (giving up for personal information such as location and driving speed) against benefits (such as navigation support).

Technological determinism holds that technology has the ability to shape our lives. Perusco et al. (2006) put forward that the social setting in which the technology emerges is as important as the technology itself. Winner (1986, p.51) believes this position can be countered when there is a clear form and limits on the idea of what a society should be. In terms of lifeworld, there is a linking of technology acceptance and shaping of social evolution. A society wishing to structure and direct its forward progress must be aware of the implications of technology in terms of costs and benefits. Without this knowledge, there is the presupposed position of the technology driving social change and not vice versa. Winner (1986, p.68) quotes Marcuse for the joining of the concept of freedom to technical progress of the advancement of science. The position he takes is that at present, the structures around the development of technology are not supportive of inclusion of lifeworld response. They are rarely designed as technologies of liberation. Michael and Michael pose the same question of balance in terms of the attempt to make the world safer through the use of surveillance cameras and the equipping of children with tracking devices. The consideration here again is whether privacy and freedom are being sacrificed, but they note that:

> …more and more people are willing to pay this price as heinous crimes become common events in a society that should know better (Michael and Michael 2004, p.441).

This society is being shaped through many influences particularly in this era of 'real and present danger' of terrorism and biological, nuclear, chemical and radiological threat. The plea in the article is that these and other implications should be considered

in the development stages of technology innovation, not after they are already in place, unable to be changed easily.

Louie and Eckhartsberg (2006, p.70) dispute that a trade-off takes place or even needs to take place. Using the example of data mining they suggest that there are at least five choices that can be made during the process that make a trade-off unnecessary. The weakness here is that these choices rely on individual reasoning looking beyond the self, to the wider implications. Voluntary codes of practice are put forward as an example where this level of decision making has failed, and their fear is that the same will happen in the context of data mining and invasion of liberties.

Westin (2006, p.19) proposes two models from which governments and the wider public are operating (see Table 5).

Table 5: Westin's Security-First and Liberty-First Models

Security First Position	Liberty First Position
If we do not modify some of our traditional constitutional norms limiting government powers, we will not be able to fight terrorism, function as a reasonably safe society and enjoy our liberties.	If we reduce our liberties by granting the government sweeping and uncontrolled investigative and surveillance powers, we will weaken the constitutional system that has made our nation great.

Westin (2006, p.20) believes there are five factors shaping public views in regard to the security versus liberty dichotomy: perceptions of the current terrorist threat and the likelihood of further attacks; perceptions of how well the government is dealing with the threats thus far and the methods being used; perceptions of how government antiterrorist programs are affecting valued civil liberties; underlying orientations toward general security and liberty issues; and basic orientations on political issues in general – which may be shaped by political philosophy, party identification, and demographic factors.

Luban (2005) builds from this consideration framework to personalise the issue more strongly. He strongly supports the notion that a trade-off is taking place and asks what "you" are willing to sacrifice in order to have "minute increments in security". Luban believes that if the trade-off question is always asked in terms of personal rights, answers may be significantly different to when the questions remain a vague societal generality. He challenges the use of September 11 as the measuring stick by which trade-off questions should be asked:

> …we would be willing to sacrifice a lot of liberty to prevent September 11…what sacrifice of our rights would we be willing to undergo to reduce the already-small probability of another September 11 by a factor of, say, one in ten? (Luban 2005, p.243).

Northhouse (2006, p.5) and Wran (2006) support these notions, prompting us to consider the role of technology in understanding the trade-off concerns, and also

recognising the impact and increasing pervasiveness of government in control of personal information.

6 Conclusion

It was stated at the beginning of this paper that location-based services and auto-ID technologies were being used for national security purposes and that their use has a social impact. By examining the technologies currently being used in the area, and also technologies being proposed for national security applications, it was shown that much of the research is happening in technology silos. There is scant research drawing together the technologies in order to understand the impact they have when used collectively for national security purposes.

This paper also established an understanding of the social dimensions of the technology which can sometimes be regarded as consequences of its use. The impact of these technologies on privacy is often discussed from a negative perspective. Although the concepts of privacy, security and liberty intersect to a degree, their interplay with regard to technology use in for national security purposes has been skewed toward the impact of terrorism. The literature on privacy and technology is dominated by works that focus on a threatening impact. This is contrasted with the security literature which proposes technology to be a fix for security concerns. The concept of liberty is manifold, and in the context of technology and national security is seemingly an emotional and tending toward biased patriotism and it seems that a choice must be made: security before liberty, or liberty before security.

The unguarded acceptance of technology as we move through various phases toward an information society, is a trend that has been inevitable, and yet still sinister. We have reached a point in the development of technologies where it is prudent to sit back and look at the potential impacts of what we are designing. Technology for the sake of technology no longer holds importance for the emerging generation. The integration of automatic-identification with location-aware technology has significant benefits for the national security area. Promotion of a technology without consent from the population may be understandable necessity in times of crisis, but the cloak of national security and the associated imminent danger is wearing thin. Technology alone will not prevent terrorist attacks. What it will do is assist society in managing these events when they do happen. Requiring society to remain on elevated levels of alert, or to be 'alert but not alarmed', propagates fear and insecurity. This serves a purpose if the theatre of security can be boosted by the adoption of a technology, however, without democratic debate; this method of technology adoption does little to liberate populations (Brzezinski 2004, p.243).

References

Acharya, A. 2002, 'State-Society Relations: Reordering Asia and the World After September 11', in K. Booth and T. Dunne (eds), *World in Collision: Terror and the Future of Global Order*, Palgrave, London.

Albrecht, K. & McIntyre, L. 2005, *Spychips: how major corporations and government plan to track your every move with RFID*, Nelson Current, Nashville.

Alippi, C. & Vanini, G. 2004, 'A genetic-based application oriented approach to optimize RFID-like passive sensor devices for homeland security', in *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety*, Venice, Italy, 21-22 July 2004

Alterman, A. 2003, ''A piece of yourself': Ethical issues in biometric identification', *Ethics and Information Technology*, vol.5, no.3, p.139.

Ames, R. 1990a, 'Opportunities and Challenges', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.6.1-6.11.

Ames, R. 1990b, 'RF Prophecy', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.5.2-5.6.

Ames, R. 1990c, 'RF/ID systems', in R. Ames (ed.), *Perspectives on Radio Frequency Identification: what is it, where is it going, should I be involved?*, Van Nostrand Reinhold, New York, pp.3.1-3.9.

Angell, I. & Kietzmann, J. 2006, 'RFID and the end of cash?' *Communications of the ACM*, vol.49, no.12, pp.91-96.

Antonioni, M. (1966). Blowup.

Ashbourn, J. 1994, 'Emerging technology for security and control', *Sensor Review*, vol.14, no.4, p.3.

Atkinson, W. 2004, 'Tagged: the risks and rewards of RFID technology', *Risk Management*, vol.51, no.7, p.12.

Barr, T. 1994, 'Australia's information society: clever enough?' in R. Guinery and L. Green (eds), *Framing technology : society, choice and change*, Allen & Unwin, St Leonards.

Bennett, C.J. 1996, 'The public surveillance of personal data: a cross-national analysis', in D. Lyon and E. Zureik (eds), *Computers, Surveillance and Privacy*, University of Minnesota Press, Minneapolis.

Bergman, C. 2005, 'Thai smart ID card ready to roll', *Biometric Technology Today*, vol.13, no.5, pp.1-2.

Borriello, G. 2005, 'RFID: Tagging the world', *Communications of the ACM*, vol.48, no.9, pp.34-37.

Branscomb, A.W. 1994, *Who owns information?: from privacy to public access*, BasicBooks, New York.

Brzezinski, M. 2004, *Fortress America: On the Front Lines of Homeland Security, An Inside Look at the Coming Surveillance State*, Bantam Books, New York.

Chabrow, E. 2005, 'Homeland security to test RFID tags at U.S. borders', *Information Week*.

Chandra, A. & Calderon, T. 2005, 'Challenges and constraints to the diffusion of biometrics in information systems', *Communications of the ACM*, vol.48,

no.12, pp.101-106.
Chaum, D. 2000, *Smartcard 2000*, Elsevier Science Publishers, Amsterdam.
Chirillo, J. & Scott, B. 2003, *Implementing Biometric Security*, Wiley Publishing Inc., Indianapolis, Indiana.
Clarke, R. 1988, 'Information technology and dataveillance', *Communications of the ACM*, vol.31, no.5, pp.498-512.
Clarke, R. 1997, *Introduction to dataveillance and information privacy, and definitions of terms*, accessed 2 June 2006, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro
Cohen, J. 1994, *Automatic Identification and Data Collection Systems*, McGraw-Hill, London.
Coppola, F.F. (1974). The Conversation.
Davies, S. 1996, *Monitor*, Pan, Sydney, NSW.
Davies, S. 1998, 'Biometrics: A Civil Liberties and Privacy Perspective ', *Information Security Technical Report*, vol.3, no.1, pp.90-94.
Day, K. (1985). Perspectives on Privacy: a Sociological Analysis. Edinburgh, University of Edinburgh.
De Niro, R. (2006). The Good Shepherd.
Eckfeldt, B. 2005, 'What does RFID do for the consumer?' *Communications of the ACM*, vol.48, no.9, pp.77-79.
El-Rabbany, A. 2002, *Introduction to GPS: the global positioning system*, Artech House, Inc., Boston.
Elliot, M. 2003, 'They had me at Prada', *Industrial Engineer*, vol.35, no.11, p.6.
Ellul, J. 1965, *The Technological Society*, Johnathan Cape, London.
ESRI. 2007, *Case Studies*, accessed 2 June 2007, http://www.esri.com/showcase/case-studies/index.html
Fincher, D. (2002). Panic Room.
Flaherty, D.H. 1989, *Protecting privacy in surveillance societies : the Federal Republic of Germany, Sweden, France, Canada, and the United States*, University of North Carolina Press, Chapel Hill.
Floerkemeier, C. & Lampe, M. 2004, 'Issues with RFID usage in ubiquitous computing applications', *Pervasive Computing*, Springer Berlin / Heidelberg, pp.188-193.
Friedrick, J. 2003, 'Homeland Security initiatives should boost the GPS market', *Security Systems News*, vol.6, no.4, p.51.
Gandy, O.H.J. 1993, *The Panoptic Sort: A political economy of personal information*, Westview Press, Boulder, Colorado.
Garfinkel, S.L. 2000, *Database nation : the death of privacy in the 21st century*, O'Reilly, Beijing.
Garfinkel, S.L., Juels, A. & Pappu, R. 2005, 'RFID privacy: an overview of problems and proposed solutions', *IEEE Security & Privacy Magazine,*, vol.3, no.3, pp.34-43.

Getting, I.A. 1993, 'Perspective/navigation-The Global Positioning System', *IEEE Spectrum*, vol.30, no.12, pp.36-38, 43-47.

Goldstone, R. 2005, 'The tension between combating terrorism and protecting civil liberties', in R. Wilson (ed.), *Human Rights in the War on Terror*, Cambridge University Press, Cambridge, pp.157-168.

Gotleib, C.C. & Borodin, A. 1973, *Social issues in computing*, Academic Press, New York.

Gunther, O. & Spiekermann, S. 2005, 'RFID and the perception of control: the consumer's view', *Communications of the ACM*, vol.48, no.9, pp.73-76.

Haneke, M. (2005). Cache.

Harris, A.J. & Yen, D.C. 2002, 'Biometric authentication: assuring access to information', *Information Management & Computer Security*, vol.10, no.1, p.12.

Hitchcock, A. (1954). Rear Window.

Howitt, P. (2001). Antitrust.

Hsi, S. & Fait, H. 2005, 'RFID enhances visitors' museum experience at the Exploratorium', *Communications of the ACM*, vol.48, no.9, pp.60-65.

IIE Solutions 2002, 'Florida airport gets first RFID system', *IEE Solutions*, vol.34, no.7, p.14.

Jain, A., Hong, L. & Pankanti, S. 2000, 'Biometric Identification', *Communications of the ACM*, vol.43, no.2, p.90.

Jayakumar, S. & Senthilkumar, C. 2005, 'Biometric fingerprints based radio frequency identification', in P. Kantor, G. Muresan, F. Roberts, D. D. Zeng, Fei-YueWang, H. Chen and R. C. Merkle (eds), *Intelligence and Security Informatics*, Springer-Verlag Berlin Heidelberg, pp.666-668.

Johnson, M.L. 2004, 'Biometrics and the Threat to Civil Liberties', *Computer*, vol.37, no.4, pp.90-92.

Jones, P., Clarke-Hill, C., Hillier, D., Shears, P. & Comfort, D. 2004, 'Radio Frequency Identification in retailing and privacy and public policy issues', *Management Research News*, vol.27, no.8/9, p.46.

Juels, A. 2006, 'RFID security and privacy: a research survey', *IEEE Journal on Selected Areas in Communications*, vol.24, no.2, pp.381-394.

Kelly, E.P. & Erickson, G.S. 2005, 'RFID tags: commercial applications v. privacy rights', *Industrial Management + Data Systems*, vol.105, no.5/6, p.703.

Kim, H.-J. 1995, 'Biometrics, is it a viable proposition for identity authentication and access control?' *Computers & Security*, vol.14, no.3, p.205.

Kinsella, B. 2003, 'The Wal-Mart factor', *Industrial Engineer*, vol.35, no.11, p.32.

Kun, L. 2004, 'Technology and policy review for homeland security', *IEEE Engineering in Medicine and Biology Magazine*, vol.23, no.1, pp.30-44.

Langford, D. (ed.) 2000, *Internet ethics*, Macmillan, Basingstoke.

Legner, C. & Thiesse, F. 2006, 'RFID-based maintenance at Frankfurt airport', *IEEE Pervasive Computing*, vol.5, no.1, pp.34-39.

"liberty n." (2004). *The Australian Oxford Dictionary*. B. Moore. Oxford, Oxford

University Press.
"liberty" (1996). *The Oxford Dictionary of Philosophy*. S. Blackburn. Oxford, Oxford University Press.
Louie, G. & von Eckhartsberg, G. 2006, 'Security and liberty: how technology can bridge the divide', in C. Northouse (ed.), *Protecting What Matters: technology, security, and liberty since September 11*, Brookings Institute Press, Washington D.C., pp.63-73.
LSE (2005). The Identity Project: An assessment of the UK Identity Cards Bill & its Implications. London, London School of Economics and Political Science.
Luban, D. 2005, 'Eight fallacies about liberty and security', in R. Wilson (ed.), *Human rights in the War on Terror*, Cambridge University Press, Cambridge, pp.242-257.
Lynch, D. (1997). Lost Highway.
Lyon, D. 2002, 'Surveillance in cyberspace: the Internet, personal data, and social control', *Queen's Quarterly*, vol.109, no.3, pp.345-357.
Mann, M. (2004). Collateral.
McLean, D. 1995, *The Difficulty of Privacy as an Idea. Privacy and its Invasion*, Praeger Publishers, Westport.
Michael, K. & Masters, A. 2006, 'Realized applications of positioning technologies in defense intelligence', in H. Abbass and D. Essam (eds), *Applications of Information Systems to Homeland Security and Defense*, Idea Group Publishing, Hershey, pp.196-220.
Michael, K., McNamee, A., Michael, M.G. & Tootell, H. 2006a, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS', in *Proceedings of the International Symposium on Technology and Society*, New York, IEEE Computer Society, 8-11 June 2006a
Michael, K. & Michael, M.G. 2004. 'The social, cultural, religious and ethical implications of automatic identification.' *Proceedings of the Seventh International Conference in Electronic Commerce Research*, Dallas, Texas.
Michael, K. & Michael, M.G. 2006a, 'The proliferation of identification techniques for citizens throughout the ages', in K. Michael and M. G. Michael (eds), *First Workshop on the Social Implications of National Security*, University of Wollongong, Wollongong, pp.7-26.
Michael, K., Michael, M.G., Tootell, H. & Baker, V. 2006b, 'The hybridization of automatic identification techniques in mass market applications: towards a model of coexistence', in *Third International Conference on Management and Innovation*, Singapore, IEEE Computer Society, 21-23 June 2006b
Michael, M.G. & Michael, K. 2006b, 'National Security: The Social Implications of the Politics of Transparency', *Prometheus*, vol.24, no.4, pp.359 - 363.
Nath, B., Reynolds, F. & Want, R. 2006, 'RFID Technology and Applications', *IEEE Pervasive Computing*, vol.5, no.1, pp.22-24.
Ng-Kruelle, G. & Swatman, P. 2002, 'The price of convenience: privacy and

mobile commerce', *Quarterly Journal of Electronic Commerce*, vol.3, no.3, pp.273-285.
Niccol, A. 1997, 'Gattaca'.
Northouse, C. (ed.) 2006, *Protecting What Matters: technology, security, and liberty since September 11*, Brookings Institute Press, Washington D.C.
Oderwald, R.G. & Boucher, B.A. 1997, *Where in the World and What? An Introduction to Global Positioning Systems*, Kendall Hunt Publishing Company, Dubuque.
OFPC (2006). Information Technology and Internet Issues. Office of the Federal Privacy Commissioner.
Ohkubo, M., Suzuki, K. & Kinoshita, S. 2005, 'RFID privacy issues and technical challenges', *Communications of the ACM*, vol.48, no.9, pp.66-71.
Orwell, G. 1949, *Nineteen eighty-four: a novel*, Secker and Warburg, London.
Peckinpah, S. (1983). The Osterman Weekend.
Perusco, L., Michael, K. & Michael, M.G. 2006, 'Location-based services and the privacy-security dichotomy', in *Third International Conference on Mobile Computing and Ubiquitous Networking*, London, 11-13 October 2006
Petersen, J. 2001, *Understanding surveillance technologies: spy devices, their origins & applications*, CRC Press, New York.
Poessl, S. 2006, *Indonesian Government unveils the World's most comprehensive, decentralized, biometric Passport Project, delivered by Digital Identification Solutions* accessed 4 August 2007, http://www.findbiometrics.com/press-release/3440
Rankl, W. & Effing, W. 2000, *Smart Card Handbook*, John Wiley, Chichester, England.
Relyea, H.C. 2002, 'Homeland security and information', *Government Information Quarterly*, vol.19, no.3, pp.213-223.
Robinson, P.A. (1992). Sneakers.
Rood, E.P. & Hornak, L.A. 2003, 'Are you who you say you are?' *The World & I*, vol.18, no.8, p.142.
Rule, J., McAdan, D., Stearns, L. & Uglow, D. 1980, *The Politics of Privacy*, Elsevier Science Publishers, New York.
Scheeres, J. 2005, 'When your mole betrays you', *Wired News*, no.19 September.
Schoeman, C. 1992, *Privacy and Social Freedom*, Cambridge University Press, New York.
Scorsese, M. (2006). The Departed.
Scott, T. (1998). Enemy of the State USA.
Smith, L. 2005, 'RFID Report', *The Humanist*, vol.65, no.3, p.37.
Snow, D. 2004, *National Security for a New Era: Globalization and Geopolitics*, Pearson Education, Inc., New York.
Spielberg, S. (2002). Minority Report.
Srivastava, L. 2007, 'Radio frequency identification: ubiquity for humanity', *info*, vol.9, no.1, pp.4-14.

Starner, T. 2001, 'The challenges of wearable computing: Part 2', *IEEE Micro*, vol.21, no.4, pp.54-67.

Swartz, N. 2004, 'Tagging toothpaste and toddler', *Information Management Journal*, vol.38, no.5, p.22.

The Royal Academy of Engineering (2004) "Response to the House of Commons Transport Select Committee: Inquire into Galileo." September 2004, accessed 4 August 2007, http://www.raeng.co.uk/news/publications/list/responses/galileo.PDF

van der Ploeg, I. 1999, 'The illegal body: 'Eurodac' and the politics of biometric identification', *Ethics and Information Technology*, vol.1, no.4, pp.295-302.

Want, R. 2004, 'Enabling ubiquitous sensing with RFID', *IEEE Computer*, vol.37, no.4, pp.84-86.

Warren, S.D. & Brandeis, L.D. 1890, 'The right to privacy', *Harvard Law Review*, vol.4, no.5, p.193.

Washington, D. (2006). Deja Vu.

Weir, P. (1998). The Truman Show.

Wenders, W. (1997). The End of Violence.

Westin, A.F. 1967, *Privacy and Freedom*, Atheneum, New York.

Westin, A.F. 2006, 'How the public sees the security-versus-liberty debate', in C. Northouse (ed.), *Protecting What Matters: Technology, Security, and Liberty since September 11*, Brookings Institute Press, Washington D.C., pp.19-38.

Wigan, M. & Clarke, R. 2006, 'Social Impacts of Transport Surveillance', in K. Michael and M. G. Michael (eds), *First Workshop on the Social Implications of National Security*, University of Wollongong, Wollongong, pp.27-44.

Winner, L. 1986, *The whale and the reactor: a search for limits in an age of high technology* University of Chicago Press, Chicago.

Woodward Jr, J. 1997, 'Biometrics: privacy's foe or privacy's friend?' *Proceedings of the IEEE*, vol.85, no.9, pp.1480-1492.

Woodward Jr, J. (2001) "Biometrics: facing up to terrorism." *RAND Issue Paper*, accessed 2 February 2006, http://www.rand.org/pubs/issue_papers/IP218/

Wran, N. 2006, *Civil liberties: an endangered species*, accessed 1 March 2007, http://lionelmurphy.anu.edu.au

Yeo, V. 2006, *S'pore unveils new biometric passport*, accessed 4 August 2007, http://www.zdnetasia.com/news/security/0,39044215,39346963,00.htm

Zoreda, J.L. & Oton, J.M. 1994, *Smart cards*, Artech House, Inc., Massachusetts.