1-1-2005

Electronic surveillance post 9/11

Chun-Lung Tai
University of Wollongong

Electronic surveillance post 9/11

Abstract

This paper examines the legal and practical issues surrounding electronic surveillance systems implemented since the September 11th 2001 terrorist attacks in three countries: the United States of America, Singapore and Australia. The paper determines their effectiveness on border security, particularly at airports. Notably, the response of each country has been influenced by its cultural structure. Central to advanced security technologies is the field of biometrics.

Keywords

Electronic, surveillance, post

Disciplines

Law

Publication Details

C. Tai, "Electronic surveillance post 9/11" (2005) 1 Rhizome 89-110.

Electronic surveillance post '9/11': the future of biometrics

Toshitatsu Tai CENTRE for TRANSNATIONAL CRIME PREVENTION

This paper examines the legal and practical issues surrounding electronic surveillance systems implemented since the September 11th 2001 terrorist attacks in three countries: the United States of America, Singapore and Australia. The paper determines their effectiveness on border security, particularly at airports. Notably, the response of each country has been influenced by its cultural structure. Central to advanced security technologies is the field of biometrics.

Rhizome 1, 89-110 (2005)

Introduction

The vast changes in surveillance implemented after the September 11, 2001 terrorist attacks have both legal and technical characteristics. The United States of America and several other countries have passed legislation to tighten security, giving police and intelligence services greater powers and permitting faster political responses to terrorist attacks. These countries have also upgraded surveillance exercises in their critical border-control strategies.

Sweeping legislative changes and broad anti-terror laws have effectively sanctioned powerful surveillance methods. As a result, technological responses to September 11 have proliferated. Current surveillance-related responses to September 11 include iris scans at airports (implemented in Europe and North America), enhanced closed circuit television (CCTV) cameras in public places with facial recognition capabilities and DNA databanks used to store genetic information capable of identifying known terrorists. Evidently, surveillance is no longer a technology used merely for controlling mobility. Biometrics security technologies, including fingerprint, face, and iris systems, are at the forefront. However, while such technologies undoubtedly aid security, the negative impact of such advances is their invasiveness upon privacy.

Background

In the wake of the September 11, 2001 terrorist attacks in the US, contemporary society has witnessed a proliferation of surveillance technology. Such advancements are essentially aimed at making the world a safer place but have invaded many aspects of daily life. For example, the president of one security firm suggested that 'every American could be given a smart card so, as they go into an airport or anywhere, we know exactly who they are.'[1] Central to the advancement of surveillance technologies is the advent of biometrics.

Modern biometrics can automate the identification of people by measuring and analysing one or more of their distinct physical or behavioural characteristics. Biometric identification systems are essentially pattern recognition systems that use acquisition devices such as cameras and scanning devices to capture images, recordings or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics. Some biometric systems require the subject's approval, however others operate passively or covertly, analysing data without the subject's knowledge. As the process is automated, biometric decision-making is generally immediate, in most cases taking only a few seconds in real time.[2]

Data used in biometrics can be encrypted, ensuring its security. Moreover a person's physical characteristics are unique and unlike identification cards and passwords they are not easily lost, stolen, counterfeited or otherwise compromised. Hence, theoretically, biometrics represents a more efficient approach to security than previous surveillance methods.[3] There are four main categories of biometric surveillance technologies:

1) Fingerprinting: based on the graphical, flow-like ridges of the fingers, systems can provide a match for fingerprints in less than two hours.[4]

2) Facial imaging: a group of methods designed to reduce facial qualities to mathematical abstractions.

3) Hand geometry: creates mathematical pattern abstractions using data derived from 96 measurements of the hand.

4) Eye scanning: An iris scan uses an infrared light to create mathematical abstractions of patterns in the coloured tissue around the centre of the eye which has approximately 266 distinctive characteristics. Retinal scanning is similar, but analyses the patterns of veins occurring in the back of the eye.

While the benefits of such technologies are evident and the potential for their expansion foreseeable, it should be noted that biometrics is a young technology having only recently reached the point where basic matching performance can be achieved. Weaknesses in the security process, environmental conditions or failures by people to operate the technology can diminish its effectiveness. Similarly, the technology itself is not infallible and errors may sometimes occur.[5] Furthermore, not all people can enrol in a biometrics system. Failure to enrol may stem from an insufficiently distinctive biometric sample or poor system design.

The US security environment

In 1974 Congress took significant steps for national security by implementing the Anti-hijacking Act and the Air Transportation Security Act. Both acts focused on hi-jacking and imposed penalties of 20 years imprisonment or death for carrying weapons or explosives aboard an aircraft. Screening of passengers and baggage was authorised.[6] During the 1980s and 90s, the US government mandated more stringent risk assessment, airline employees' background checks and passenger profiling with the enactment of four more critical pieces of legislation: the Foreign Airport Security Act of 1985; the Aviation Security Improvement Act of 1990; the Federal Aviation Administration Reauthorisation Act of 1996; and the Aviation Security Improvement Act of 2000.

When congress conferred comprehensive jurisdiction for aviation security on the Department of Transportation (DOT), the DOT was made responsible for regulating the screening of passengers and property, dealing with threats to domestic and international civil aviation, establishing security standards at foreign airports, issuing travel advice, the requirement of passenger manifests, providing airport construction guidelines, and fostering an accelerated program of security research and development including explosive detection.[7]

Despite these measures, the events of September 11 poignantly revealed the vulnerability of the U.S. civil transportation system which was totally unprepared for these attacks. Dempsey analysed four key factors which could be deemed as vulnerabilities:

1) The porous transportation security umbrella;

2) The undue reliance on a single mode of transportation;

3) A significant reliance on the transportation industry for America's economy;

4) Poor or nonexistent internodal connectivity.[8]

The 9/11 Commission also criticised the fact that no agency of the U.S. government systematically analysed terrorists' travel strategies. There was a lack of well-developed counterterrorism measures as a part of border security and the inept immigration system was not able to deliver on its basic commitments, much less support counterterrorism.[9]

The government swiftly undertook sweeping legislative reform on terrorism and national security in the aftermath of 9/11. This campaign was headed by the USA PATRIOT Act ('Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001'), which along with the Border Security Bill was designed to strengthen US borders, broaden the power of law enforcement agencies and secure the visa entry system.[10] The USA PATRIOT Act permits greater sharing of intelligence information between law enforcement and national security investigators, regardless of the source of the intelligence information.[11]

In relation to aviation security, Congress federalised airport screening functions, establishing the new Transport Security Administration (TSA)[12] under the DOT.

The TSA became responsible for regulating security in all modes of transportation, imposing minimum job qualifications upon security employees, performing background checks on airport employees, research and development, screening passengers, baggage and cargo, assessing security threats, hiring security personnel, maintaining security facilities,[13] as well as requiring the installation of impregnable cockpit doors via the Aviation and Transportation Security Act of 2001.[14] The TSA also implemented the Computer Assisted Passenger Pre-Screening (CAPPS) system with the aim of improving their ability for profiling. Notably this implementation involved amendments to the U.S. Privacy Act. Finally, Congress enacted the Homeland Security Act of 2002, thus consolidating twenty-two agencies and creating the Department of Homeland Security which was given jurisdiction, inter alia, over transportation security, customs, immigration and agricultural inspections. Some anti-terrorism efforts, including those involving access control to secure areas and identifying travellers, include biometric technologies.[15]

Various technological initiatives have been employed to meet new Congressional mandates and comply with recent legislative reforms. By way of illustration, to allow for the screening of all bags at U.S. airports, between 4000 and 6000 Explosive Detection System machines were to be installed at 429 airports in the U.S.[16] San Francisco International Airport has employed hand geometry devices in conjunction with identification cards to protect secure areas of the airport, such as the tarmac and loading gates. In 2003, Toledo (Ohio) Express Airport also installed hand geometry devices while Chicago's O'Hare International Airport required smart cards and fingerprint recognition to control access to cargo areas.[17]

CCTV has also become one of the main modes of surveillance within airports. This has allowed for the expansion of facial recognition technology and sophisticated tools such as the 'FaceIt' system which enables a standard PC to scan 70 million images per minute.[18]

Other examples of advanced surveillance devices based on biometric-technologies include the Trusted or Registered Traveller Program whereby a frequent flyer who provides the TSA with background information, later receives a biometrically enabled ID card. A further example is that of the National Security Entry-Exit Registration System (NSEERS) which was implemented at several points of entry on September 11, 2002. The initiative requires fingerprinting and photographing of all visitors to the U.S. at all U.S. borders, periodic registration of immigrants who stay in the country for more than 30 years and exit controls enabling officers to arrest people who overstay their visas.[19] Moreover, in 2002 the White House

was involved in establishing modern visa systems based on sharing biometric information between federal databases as well as a computerised entry-exit system ensuring visitors comply with their entry conditions.

The Singaporean security environment

Singapore achieved self-government with independence in 1965 and has borne the stamp of the People's Action Party (PAP) rule for over forty years. Regarded as a safe and orderly nation it was one of the first places to adopt new ideas for increasing security efficiency.

Prior to the 9/11 attacks, Lee Kuan Yew, the long ruling Prime Minister largely responsible for Singapore's economic success, instigated policy similar to the U.S. ensuring Singapore's critical locations were protected by highly sophisticated security technologies. The 'Total Defence' regime, which involves the entire citizenry in Singapore's defence, remains the cornerstone of Singapore's deterrent strategy. Furthermore Singapore has always placed cultural significance on the success of the Singapore Armed Forces (SAF) and the ideology that Singapore is capable of defending itself.

Like Australia, Singapore's post 9/11 allegiance with westernised nations has essentially made it a terrorist target. This general notion was made evident in 2002 with concerns of Islamic terrorist cells operating in Singapore. It is widely accepted that Islam is not synonymous with terrorism, however, given Singapore's multiracial population with its significant Islamic representation, it is feared that there may be opposition to international anti-terrorism campaigns originating from the U.S.[20]

In response to the 9/11 terrorist attacks, Singapore strengthened its anti-terrorist efforts by passing laws such as the Terrorism (Suppression of Financing) Act in 2002, that codify United Nations resolutions relating to the funding of terrorist activities and making false terrorist threats. This legislative reform has been financially backed by the government. For example, the budget for homeland security reached $2.35 billion for 2004, representing a rise of 1.5% over 2003 and a jump of more than 10% over 2002.[21]

Additionally in response to internal and external terrorist threats, Singapore allocated additional funds to enlarging the SAF and the police force and has set up a new homeland security framework.[22] Furthermore the new National Civil Aviation Security Committee protects Changi Airport from terrorist attacks by overseeing security procedures such as baggage security and restriction of access.[23] Immigration officers at airports have also been given increased powers to direct and detain any suspect person entering the country.[24]

The Immigration and Checkpoints Authority (ICA) in charge of border security announced two projects aimed at being ready by last year: a $9 million system linking land, sea, and air checkpoints electronically; and a $400,000 land checkpoint system that can clear travellers, screen vehicles and collect toll charges. Another project is biometric passports, which involve the scanning of personal characteristics like fingerprints and iris features onto a mobile computer chip.[25] Furthermore, in 2004 the Minister of State and Transport, Balaji Sadasivan, announced that a new biometric-based security system would be tendered. Another such project is the new $80 million baggage screening system which was being implemented in late 2004.[26] Currently the government is employing a fingerprinting machine in its border control strategy capable of matching print images in less than a minute.[27]

In 2003 another issue arose mandating the government implement advanced security systems at the international airport. In April 2003, Singapore added SARS to the Quarantine Act, a law which had previously been dormant for 27 years. Measures taken to combat SARS included 'contact tracing' and the thermal-image detection of body temperatures in public places.[28] The relevant technology, Infrared Fever Scanning System (IFSS) was developed in Singapore and is currently used in more than fifty countries. Security cameras and electronic wristbands are also used to quarantine affected individuals. [29]

The Australian security environment

The series of events on September 11th 2001 impacted on national security systems in Australia. This impact was compounded by the tragic bombing in Bali on October 12th 2002. Prior to these two attacks, the use of surveillance devices by Commonwealth, State and Territory law enforcement agencies was regulated by a patchwork of divergent legislation.[30] However following the bombings in Bali, the federal government announced that it would seek a transfer from the states of their power to legislate in respect of counter-terrorism.[31]

The New South Wales Law Reform Commission concluded that 'device specific' legislation would be impractical, requiring constant updating as technological developments inevitably outpace the law.[32] It also concluded that regulating particular electronic devices was arbitrary, when surveillance could also be conducted through the use of other equipment it described as electro-magnetic, acoustic and mechanical.[33] Finally, it has been acknowledged that the power of detention is an intelligence exercise based on universalised surveillance targeting an entire population. The notion of universalised surveillance itself has created an environment in which nothing can remain private.[34]

Australia has introduced a raft of legislative measures post 9/11 including:

1) the Security Legislation Amendment (Terrorism) Act 2002, which updated and expanded the offence of treason, and created new terrorism offences;

2) the Suppression of the Financing of Terrorism Act 2002, which created and offence directed at those who provide or collect funds for intentioned terrorist activities and required cash dealers to report transactions that are suspected to relate to terrorist activities;

3) the Criminal Code Amendment (Suppression of Terrorist Bombing) Act 2002, which created new offences for placing or detonating an explosive or other lethal device with the intention of causing death or serious harm;

4) the Telecommunications Interception Legislation Amendment Act 2002, which allowed law enforcement to intercept electronic communications without a warrant; and

5) the Border Security Legislation Amendment Act 2002, which required airlines to provide Customs with access to their computer reservation systems in order to help identify high risk passengers.[35] Under the new Customs Legislation Amendment and Repeal (International Trade Modernisation) Act 2001, cargo carriers are required to report their cargo before arrival.[36]

Furthermore the amended Criminal Act of 1995 now relates to any offence against UN counterterrorism instruments. The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004 aims to ensure that Commonwealth criminal offences remain effective in the modern telecommunications environment and continues the government's proactive approach to updating criminal laws in light of rapid technological change.[37] Another example of this is the Australian Passports Bill 2004 which, not only creates stricter penalties, but for the first time considers the application of biometrics in passports.[38]

In 2002 the Commonwealth government committed $2.1 billion to ensure upgraded security, secure borders and strengthened defence forces.[39] The Budget provided an additional $539 million to the Australian Federal Police (AFP), Australian Protective Service (APS) and Australian intelligence agencies to promote increased screening of imported goods, enhanced cooperation with

overseas law enforcement agencies, and improvements in screening arriving and departing international passengers. APS officers provide heightened security at Australia's airports with enhanced capacity for detecting explosives. Uniformed and plain clothed officers also travel on certain flights.

As a result of new air traffic control technology, flights across Australia are likely to be safer and have fewer delays. The technology, Automatic Dependent Surveillance (Broadcast) or ADS-B will be rolled out country-wide by 2005. Other initiatives include Australia's Advanced Passenger Processing system. From 2004 the system required information on all international travellers (including crew) arriving by air or sea. Moreover, regional airports may be issued with further passenger screening equipment for use in heightened security situations under a $48 million package announced by federal government in August, 2004.[40]

Ensuring the reliability and authenticity of passports during the passenger screening process is a critical element of airport security. The 2002-3 Budget provided the Department of Foreign Affairs and Trade (DFAT) with $3 million for research and development of a biometric identifier for the Australian passport. Positive results in facial recognition research assured further funding was obtained in the 2003-04 Budget.[41] Proposed changes to the Australian Passport Act noted above will provide for the inclusion of a facial biometric indicator in new passports and strengthen the government's ability to combat identity fraud.

Future systems in Australia may see a person's passport photo used to create a detailed electronic portrait of their face using biometric technology. This portrait will then be stored on a tamper-proof microchip inside the passport. This system not only assures passport integrity but also efficiency by allowing computers to automate passport checking at border control points.[42]

In order to improve identity verification processing and reduce fraud, a facial recognition technology called 'SmartGate' is also being trialled. This system is advocated due to its less invasive methods, as essentially no physical contact need occur between the passenger, machine or officer.[43] Another development, known as the IP@SS (Integrated Passenger Security Solutions) system involves biometric data and passenger profiling being incorporated into a 'smart card' which may be applied for in advance, lessening processing time at the airport.[44]

The government's pro-active stance in relation to biometrics at airports has resulted in Australia meeting international technological benchmarks. Armed with new legislation and a funding commitment, following international compatibility trials and further development, Australia will be in a strong position to implement

biometrics.[45] The implementation of modern surveillance equipment will give law enforcement bodies greater power to detect illegal cross border activities and successfully prosecute offenders.[46] Moreover, new legislation amending the Migration Act 1958, will allow for more efficient identification of non-citizens by providing a clear framework for the collection of biometric identity information (including fingerprints, facial and iris recognitions).[47]

Examination of the biometric-based electronic surveillance systems

As illustrated above, each of the three countries has recently implemented stronger surveillance measures incorporating advanced technology and biometrics. However, modern circumstances have also witnessed crowded transportation facilities like airports becoming attractive targets for terrorist attacks.[48] Biometrics have the potential to prevent this by ensuring accurate identification, a cornerstone of security and the essence of countering identity fraud. Another key advantage of biometrics is that they invariably focus on unique attributes and are more difficult to falsify than traditional documentation. Moreover, the cost involved in integrating biometrics is decreasing.

As illustrated biometric-searches have many advantages and biometrics would generally offer a more secure airport environment. However the effectiveness of biometrics cannot be merely assumed and the following factors should be considered:

1) Eligibility criteria for biometric programs;

2) The content of background checks to certify eligible applicants for enrolment in a program;

3) Security-screening procedures for differentiating between registered travellers and unregistered travellers; and

4) The extent of privacy liability to be protected prior to the implementation.[49]

Another important feature of biometric implementation is the ability of individuals to challenge the technology[50] and related rulings such as the suspension of a passport. This factor is not only important to democracy and natural justice but also ensures effective review of the technology and will help remedy errors. Notably a major failure of any surveillance system is that despite its efficiency, its

effectiveness can only be ensured if it cannot be circumvented. For example, in the case of 9/11 attacks, the identity of each hijacker was known and each was allowed to board the plane. Even those accepted by surveillance systems may still intend to cause harm.

One feature that is essential to the success of enhanced international transportation security is international cooperation. Regardless of the efficiency of biometrics, their enduring success in counter-terrorism will necessarily involve cohesion and cooperation between different nations. Technology alone will be less effective in the absence of intentional collaboration on data sharing, as envisaged by the USA PATRIOT Act.

Regarding international collaboration post 9/11, President Bush announced: "Every nation in every region now has a decision to make: Either you are with us, or you are with the terrorists... what is at stake is not just America's freedom. There is the world's fight. There is civilisation's fight. This is the fight of all who believe in progress and pluralism, tolerance and freedom. We ask every nation to join us."[51] In addition, the 9/11 Committee recommended that the U.S. should engage other nations in developing a comprehensive coalition strategy against terrorism, with a view to targeting terrorist travel and sanctuary.[52] In accordance with this position, the U.S. recently extended the deadline for twenty-one nations in a 'Visa-Waiver Program' to begin to incorporate biometrics into passports. It suggests that the U.S. no longer feels secure and that it requires intensified cooperation from other countries particularly those known to be the home of terrorist organisations. To be successful, the U.S. needs to keep inviting, persuading and pressuring foreign governments to join with it in fighting terrorism globally.

Recent U.S. advancements have included enhanced identification systems such as the IDENT and United States Visitor and Immigrant Status Indicator Technology (US-VISIT) systems, which require visitors to the U.S. to submit a biometric identifier to the U.S. government. Systems such as these have been implemented at many entry points to the U.S., as have immigration tracking programs. As envisioned by the USA PATRIOT Act and Border Security Act the US-VISIT program was intended to be expanded to include other categories of foreign nationals. Accordingly Singapore and Australia will likely have to adapt their domestic visa policies for fear of not being able to obtain a U.S. visa. The Australian government has acknowledged as much stating that "the war on terrorism is not a battle which can be fought on one front."[53]

Effective cooperation on counter-terrorism however, involves much more than words, and the relationships between these three countries are vital. It cannot

be denied that U.S./Singapore relations have been difficult at times. However the U.S. is clearly the major power most important to Singapore and the relationship has been consistently on good terms in regards to defence diplomacy. Singapore also has long supported the presence of the U.S. in Southeast Asia and regarded it as crucial to peace and stability in the region. The two countries moved closer with the arrests in Singapore of suspected terrorists in three cells of the Jemaah Islamiah, who were apparently plotting to attack the U.S.[54] The relations between these two countries have warmed with the bilateral free trade agreement in 2003, the growth of U.S. investment in Singapore, and the large number of Singaporeans visiting and studying in the U.S. resulting in their incorporation in the Visa Waiver Program.[55]

Similar to Singapore's foreign policy, the U.S. has been recognised as an influence in Australian domestic policies. Australia is regarded as a strong ally of the U.S. and relations between these two countries have been recently secured by the bilateral free trade agreement, growth of U.S. investment in Australia and the re-election of Prime Minister Howard. Accordingly, Australia is also a Visa Waiver Program country.

One potential strategy relying on international relationships is extradition. The United Nations (UN) recognised extraditing criminals as an effective scheme against transnational organised crime including terrorism.[56] To keep suspects from fleeing prosecution in one country and reaching freedom in another, the UN suggests nations should recognise crimes as extraditable when no extradition treaty exits with the nation where the suspect is located and conclude bilateral and multilateral agreements to make extradition more effective.[57]

The U.S. currently has extradition treaties with about 111 countries including important Asian nations. Singapore has extradition legislation and furthermore where no extradition treaty is in force between Singapore and another country, the UN Convention may be applied to allow extradition.[58] Australia also has extradition legislation under which an extraditable offence is basically defined as any offence punishable in Australia.[59] Most extradition requests have been granted to the U.S.,[60] however the act was amended by the Criminal Act 2002 which ensures that offences are not regarded for the purpose of extradition as "political" offences in response to 9/11.[61]

While there appears to be a level of cooperation between these three countries, it should be noted that the Singaporean and the U.S. governments ultimately believe that national interests may at times supersede the need for cooperation.

Possible conflicts in biometric technology implementation

Current national security trends in these three countries are leaning toward stricter security laws and more invasive technology implementation. This has also been the trend elsewhere globally. However, arguably the new technologies are likely to give rise to unintended consequences that hinge on questions of legality, privacy invasion, diplomatic difficulties and the differences in cultural and moral values inherent in each country.

Issues relating to the legality of biometric-based system application

As biometrics are a relatively new technology, there is a paucity of cases which examine biometric application in legal procedure. However, there are several cases in which the legal applicability of biometric technology is mentioned, in particular in the U.S.

The Fourth Amendment to the U.S. Constitution protects "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures".[62] Courts in the U.S. have indicated that the use of advanced surveillance equipment, not generally available to the public, may warrant Fourth Amendment protection.[63] In 1989, the Supreme Court ruled that where physical evidence is collected from a person, gathering of that evidence must not intrude into the person's body and furthermore the potential to reveal private medical facts about that person must not infringe the expectation of privacy that society recognises as reasonable.[64] Given this dictate, it is often questioned whether certain biometric methods would breach the amendment.

A similar consideration is whether subjecting a person to other advanced technology such as facial recognition biometrics will violate the Fifth Amendment. While facial recognition technology has not been specifically judged, other biometric issues have arisen in the courts. For example, the use of handwriting exemplars as a means of identifying suspected criminals was found not to have violated the defendant's right against self-incrimination[65] nor did the use of voice exemplars.[66]

More recently, U.S. Courts tackled the issue of high-tech, sense-enhancing surveillance equipment. The Supreme Court determined that when "the government uses a device that is not in general public use, to explore details... that would previously have been unknowable without physical intrusion, the

surveillance is a 'search' and is presumptively unreasonable without a warrant."[67] One exception to the need for a warrant is an 'administrative search'. An administrative search is one "conducted as part of a general regulatory scheme in furtherance of an administrative purpose."[68] As Star attests, airport searches employing the use of biometrics pursuant to the ATSA fall under this definition and accordingly, biometric-based searches at airports should be exempt from the Fourth Amendment's warrant requirement.[69] However the courts have continued to assess new technologies on a case by case basis. This is important in balancing biometrics and the need for U.S. government to act within the Constitution.

Privacy issues and biometric systems

As technology advances and that which was once unique becomes commonplace, privacy standards have had to evolve in order to apply to modern technology. Biometric technology invariably involves some invasion to the individual and accordingly the advent of this type of surveillance has led to privacy concerns. The U.S. has enacted legislation for the use of biometrics such as the USA PATRIOT Act, the ATSA and the Foreign Intelligence Surveillance Act (FISA). However, at present in the U.S., the Constitution, Federal law and State privacy laws provide little in the way of privacy protection.

According to one definition privacy is the 'right to be left alone'.[70] Additionally, privacy is part of the claim to personal autonomy and arguably supports the various freedoms that democratic countries value. However, the modern trend towards enhanced security has witnessed the advent of biometric-based search technologies while governments questionably turn a blind eye to privacy. Generally an invasive action such as a personal search should be accompanied by a subjective expectation of privacy with respect to that action, however security measures in place have substantially lowered the privacy expectation in airports. [71] In some cases airport searches are reconciled with privacy rights due to the passengers consenting.[72] However, in keeping with the subjective expectation of privacy, U.S. Courts have held that passengers must have the option to leave at any point prior to or during a search.[73] Moreover while the U.S. Constitution does not specifically guarantee a right to privacy, the Supreme Court has recognised a limited right to privacy in several cases.[74] Furthermore despite their dearth at a federal level, several states have created privacy rights. For example, California has created privacy rights for its citizens and moreover has declared that privacy is an inalienable right.[75]

The U.S. Privacy Act of 1974 provides additional protection to individual privacy. The 1974 Act limits federal agencies' collection, use, and disclosure of personal information and hence generally applies to personal biometric information. However, the Act provides exemptions for law enforcement and national

security purposes.[76] Furthermore, surveillance for national security purposes is now governed by the FISA which has less rigorous requirements.[77] Similarly the USA PATRIOT Act has substantially weakened protection from wiretapping and programs such as Total Information Access (TIA) and CAPPS-II allegedly present further risks to civil liberties.[78] Amendments to The Freedom of Information Act (FOIA) allow anyone to access federal government records. However, once again there are exceptions that weaken the effectiveness of the Act. Additionally as biometrics are operated on computer systems, they have become susceptible to new threats such as hacking.[79] One method advocated to prevent the abuse of biometrics is the objective monitoring and control of the technology,[80] including public notification as seen in California.[81]

Singapore also provides regulation of privacy rights generally and more specifically in relation to data protection. For example the E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce, prohibits the disclosure of personal information, and regulates service providers.[82] Also major bills have been enacted such as the Computer Misuse (Amendment) Act which prohibits the unauthorised interception of computer communications.[83] However, due to the outbreak of SARS, the events of September 11 and the modern government's strict national security policy, legislation currently provides police with broad powers of investigation. Singapore has no constitutional right to privacy and although government officials are normally required to obtain court-issued search warrants, broad exceptions exist to this weak rule.[84]

Under the authoritarian leadership of Singapore's founding father, Lee Kwan Yew, Singapore effectively legitimised the rejection of liberal values.[85] As a result, Singapore is regarded as an almost totalitarian regime with a low value of personal privacy.[86] Citing the doctrine that 'the kind of society determines the level of privacy protection', Singapore has gained a reputation for aggressively using surveillance for social control. Reputably Lee is even proud of interfering in the private lives of citizens.[87]

In contrast, the common law in Australia provides some protection against unjustified surveillance. The laws of trespass, nuisance and defamation may provide the subject of surveillance with redress in certain circumstances.[88] Also the Privacy Acts of 1988 and 1998 have instilled strict rules on collection, use and storage of personal information including tax file numbers. However, legislative amendments in 2002 and 2003 have given ASIO significant and highly controversial new powers including the ability to detain and question individuals suspected of having information relevant to terrorism.[89]

Ultimately as Lyon argues, "although privacy laws and data-protection are very important, by themselves they remain inadequate as a means of limiting today's newly augmented surveillance power."[90] It is also argued that while personal privacy is paramount, intrusions into it by way of surveillance are sometimes necessary for the greater public benefit.[91] Dripps attests that when the unexpected cost of crime includes the loss of entire cities, the standard liberal position becomes either untenable or fanatical.[92] Hence although privacy encourages free thought and free expression and limits the reach of government power, it is inevitable that at times it will be discarded in the name of counter terrorism. The real risk to privacy however, will occur when use of biometrics are employed covertly.[93]

Diplomatic difficulty

As discussed the global nature of terrorism and potential for sharing counter-terrorism information via new technologies has made international cooperation highly desirable. However, as was also noted earlier, achieving such cooperation is seldom easy. It is argued that foreign policies that isolate, and further alienate, so-called 'rogue-states' will result in the continuance, not curtailment, of state-sponsored terrorism.[94] Furthermore, discrimination and prejudice have increased due to the religious motivation and nationality of many terrorist groups. While U.S.A./Australian/Singaporean relations are sound in these respects, vast cultural differences between Eastern nations, such as Singapore, and Western nations, such as the U.S. and Australia, have had significant affects. This point is critical in integrating international collaboration, although a detailed discussion is far beyond the scope of this legal/technological paper. Notably however, as western laws become more invasive and strict, as has been witnessed in both the U.S. and Australia, they progressively merge with Asia's more authoritarian culture.

Conclusion

As discussed, these three countries have changed their laws to address the environment following '9/11'. Each country has increased the ability of law enforcement and national security agencies to perform interception of communications, and has transformed search powers. Each country has also instigated an increase in the type of data that can be accessed via new anti-terror laws which expand surveillance authority.

For terrorists, travel documents are as important as weapons. In their travels, terrorists use altered and counterfeit passports and visas, specific travel methods and routes. Thus, increased airport security prior to boarding appears to be the most effective means of preventing politically motivated hijackings and other attacks. Therefore, as examined, biometric technologies are available today

that can be used for aviation security to detect these activities. However, it is important to keep in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work cohesively in overall security processes. To this end, programs for international cooperation that consider diplomacy, privacy rights, cultural differences and vital data sharing should be established.

The serious problem of how surveillance technology should be used remains. None of the biometric systems outlined above would have prevented the tragedy of September 11th. This is because all of the attackers already had valid identity cards with a biometric authenticator and a state-issued driver's license with a photograph. The airlines knew the identities of the attackers and allowed them to board their flights without question. What was not known was their intentions. In this paper, elements of the success of the future of surveillance, particularly biometrics, have been discussed. However, it is apparent that successful solutions must involve a vast range of measures.

REFERENCES

[1] Glaberson, W., Technology's Role to Grow in a New World of Security [online] <http://www.nytimes.com/2001/09/18/national/18RULE.html?ex=1095825600&en=78e7549931869f3d&ei=5070>.

[2] Rhodes, K.A., 2004. The Use of Biometrics to Improve Aviation Security. Hearing before the Subcommittee on Aviation, 108th Congress 2nd Session 19 May 2004.

[3] Rhodes, above n 2.

[4] For instance, the Cross Match Technologies offers its original reader, which costs about $400, records the images of two fingers and produces a match in less than a minute. Woodyard, C., 2004. Fingerprinting's big business for Cross Match Firm booms as readers go to airports all over. USA Today, 13 January.

[5] False matches may occur because there is high degree of similarity between two individuals' characteristics. False non-matches occur because there is not a sufficiently strong similarity between an individual's enrolment and trial templates.

[6] Anti-hijacking Act of 1974, Pub. L. 93-366, tit. I, 88 Stat. 409. This legislation was enacted to implement the Hague Convention, as well as to respond to the Cuban problem.

[7] 49 U.S.C. 44901-44915 (2002).

[8] Dempsey, P.S., 2003. Aviation Security: The Role of Law in the War Against Terrorism. *Columbia Journal of Transnational Law* 649, 656.

[9] The 9/11 Commission, What to do? A Global Strategy *The 9/11 Commission Report* 361, 384.

[10] Johnson, J.H. Jr, 2002. U.S. Immigration Reform, Homeland Security, and Global Economic Competitiveness in the Aftermath of the September 11, 2001 Terrorist Attacks' *North Carolina Journal of International Law & Commercial Regulation* 419, 449-450.

[11] The USA PATRIOT Act, s 219. The Freedom of Information Act also asked the DOJ to disclose information about its domestic spying since 9/11 under the USA PATRIOT Act.

[12] TSA's access control program focuses on biometrics, video surveillance, radio frequency identification (RFID) and anti-piggybacking technologies.

[13] 49 U.S.C. 114, 44901, 45107 (2002).

[14] Under the Aviation Act, federal airport security guards are not entitled to the same job protection that normally accompany civil service positions. Federal supervisors are afforded discretion to dismiss security employees; failure to screen adequately will result in dismissal.

[15] Rhodes, above n 2.

[16] Dempsey, above n 11, 727.

[17] Rhodes, above n 2.

[18] McCormack, D., 2003. Can Corporate America Secure our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Recognition Technology' *Boston University Journal of Science and Technology* 128, 131. The image is run through the software and FaceIt then creates a digital map of the extracted face, creating an identification of the person. However, there are some reports on biometric-based technologies, the International Civil Aviation Organisation (ICAO) in 2003 rated facial recognition as the most accurate biometrics identification technology, while the US-based International Biometric Group (IBG) completed a study for the Bush administration rating fingerprints as the most accurate and reliable biometrics technology, with iris recognition coming in second. 2004. Airports To Deploy Biometrics in Test Projects 11 World Airport Week 1.

[19] French, V., 'In the Age of Terror, When Is It Wrong To Require Positive Identification?' [online] <http://www.technologyreports.net/nextinterface/?articleID=867>.

[20] Ministry of Foreign Affairs Singapore, Remarks in Parliament by Singapore Foreign Minister Prof S Jayakumar on Strategic Review in the World, Including the Situation in Iraq, and Asia-Pacific Region, 14 March 2003 [online] <http://www.mfa.gov.sg/iraq.html#interest>.

[21] Gee Pek, T, 2004. The Business of Homeland Security *The Edge Singapore* 3 May 2004.

[22] Mauzy, D.K. and Milne, R.S., 2002. *Singapore Politics Under the People's Action Party* 170-171.

[23] Acharya, A., 2004. Defending Singapore's Vital Infrastructure Against Terrorism. September, *IDSS Commentaries* [online] <http://www.idsss.edu.sg>.

[24] Immigration Act, Part IV.
[25] Gee Pek T, above n 26.
[26] Ibid.
[27] Woodyard, above n 5.
[28] Paddock, R. and Effron, S., 2003. SARS Under Control in Singapore, WHO Says, Los Angels Times (Los Angeles) 1 June 2003, 4.
[29] Hoong, C.M., 2003. Govt's SARS Action Swift, But Shows Up Lack of Checks. *Straits Times*, 10 May 2003.
[30] Leaders Summit on Terrorism and Multi-jurisdictional Crime Cross-Border Investigative Powers for Law Enforcement Report, November, 2003 [online]<http://www.ag.gov.au/www/rwpattach.nsf viewasattachmentPersonal/F9182AB917673CF2CA256DE5000D1D43$file10%20Cross%20Border%20Report 2read.pdf> 345.
[31] Hocking, J., 2003. Terror Laws: ASIO, Counter Terrorism and the threat to Democracy 232.
[32] New South Wales Law Reform Commission, Surveillance: An Interim Report, Report 98 (Sydney: NSW Law Reform Commission, 2001) 44.
[33] Ibid, 44-45, 53-54.
[34] Hocking, above n 38, 233.
[35] Wright, M.A. International Terrorism Response Ignores Privacy *Computer Fraud & Security*, 14, 16.
[36] Bascombe, D., 2004. An Update of Anti Terror Legislation in the Commonwealth. [online]<http://www.humanrightsinitiative.or/new/anti_terror-legislation_cw2004.pdf> 13.
[37] Commonwealth Parliamentary Debates, House of Representatives, 4 August 2004, 31963 (Mr Rudd).
[38] Ibid, 32044.
[39] It is also because Australia operated a substantial immigration program where around 12,000 places under the humanitarian category for refugees were offered. The government does not intend to allow people smugglers to determine the intake under this program. Therefore $1,635 million has been proposed to spend on border security over five years. Peter Costello, Budget Speech 2002-03, 14 May, 2002 [online] <http://www.dfat.gov.au/budget/2002-03/budget_speech/download/Reps.pdf>.
[40] Regional Airport Security Upgrade, The Age, 23 August 2004.
[41] DFAT, Reporting against Effectiveness Indicators [online] <http://www.dfat.gov.au/dept/annual_reports/02_03/performance/2/2.1.html> 106.
[42] The Attorney-General, Support for Crime Fighting Budget 2004-2005, Fact Sheet 3 [online] <http://www.ag.gov.au/adg/www/Bidgethome2004.nsf/Page/Fact_Sheets_Docs_Fact_Sheet_3_-Border_Protection>.

[43] Maclean, G., 2003. Transcript, 5 September 2003, 70.

[44] For privacy issues, after 24 hours the personal and flight information on the IP@SS computer system would be made unreadable unless it was needed for government investigations. After 30 days it would be automatically deleted. The Parliament of the Commonwealth of Australia Joint Committee of Public Accounts and Audit, 'Report 400: Review of Aviation Security in Australia', June 2004 37, 45.

[45] Commonwealth *Parliamentary Debates*, House of Representatives, 4 August 2004, 32055 (Mr Billson).

[46] The Attorney-General, Support for Crime Fighting, Budget 2004-2005, Fact Sheet 5 [online] <http://www.ag.gov.au/adg/www/Bidgethome2004.nsf/Page/Fact_Sheets_Docs_Fact_Sheet_5_-Support_for_Crime_Fighting>.

[47] Migration Legislation Amendment (Identification and Authentication) Act 2004 coming into effect on 27 August.

[48] Szyliowicz, J.S., 2004. International transportation security, The Review of Policy Research, 1 May [online]<http://www.highbeam.com/library/doc3.asp?DOCID=1G1:116859676&num=1&ctrlInfo=Round9%3AProd%3ASR%3AResult&ao=1>.

[49] Rhodes, above n 2.

[50] Feldman, R., 2003. Considerations on the Emerging Implementation of Biometric Technology. 25 *Hastings Communications and Entertainment Law Journal* 653, 661.

[51] Satha-Anand, C., 2003. Mitigating the Success of Terrorism with the Politics of Truth and Justice. *In* Gomez, J. and Smith, A. (Ed.), *S*eptember 11 and Political Freedom: Asian Perspectives 30, 38.

[52] The 9/11 Commission, above n 9, 379.

[53] Ruddock, P., 2004. Statement by the Attorney General Philip Ruddock on National Security – overseas developments. Commonwealth, 19 February 2004 [online] <http://www.nationalsecuirty.gov.au/agd/www/nationalsecurityhome.nsf/Page/News_Media_2004_Media_Statements_Media_Transcripts_1st_Quarter_19_February_2004_The_Hon_Philip_Ruddock_MP,_Attorney-General_-_Statement_on_national_security_-_overseas_developments> 7.

[54] Mauzy and Milne, above n 22, 180.

[55] US Department of State, Bureau of East Asian and Pacific Affairs [online] <http://www.state.gov/r/pa/ei/bgn/2798.htm>.

[56] However, it is argued that "one of the most troubling issues in extradition practice is the question of the extent to which states extradite their own citizens." Harris, J. E., 2001. International Cooperation in Fighting Transnational Organized Crime: Special Emphasis on Mutual Legal Assistance and Extradition 57, *Resource Material Series* 133, 142.

[57] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 'Draft United Nations Convention against Transnational Organised Crime', Fact Sheets No 1 [online]<http://www.un.org/events/10thcongress/draft.

htm>.

[58] Terrorism (Suppression of Financing) Act 2003, Part V.

[59] Extradition Act 1988 (Cth), s 19.

[60] Australian Parliament. Joint Standing Committee on Treaties, The Parliament of the Commonwealth of Australia, Extradition: a review of Australia's law and policy (2001) 15-16.

[61] The Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002, No. 58 amended Extradition Act 1988 (Cth), s 5.

[62] U.S. Constitution. Amendment IV.

[63] Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[64] Skinner v. Railway Labour Executives' Association, 489 U.S. 602 (1989).

[65] Gilbert v. California, 388 U.S. 263 (1967).

[66] United States v. Dionisio, 410 U.S. 1 (1973).

[67] Kyllo v. United States, 533 U.S. 27 (2001). Justice Stevens stated in his dissent that the use of thermal imaging was nothing more than an extension of the plain view doctrine, which states that police are not expected to avert their eyes from evidence of criminal activity that any member of the public could have observed and that the use of the thermal imaging camera was not a search.

[68] United States v. $ 124,570 U.S. Currency, 873 F. 2d 1240 (9th Cir. 1989).

[69] Star, G., 2002. Airport Security Technology: Is the use of Biometric Identification Technology Valid Under the Fourth Amendment?. *Temple Environment Law and Technology Journal* 251, 263.

[70] Warren, S. and Louis Brandeis, The Right to Privacy [online] <http://www.louisville.edu/library/law/brandeis/privacy.html>.

[71] Katz v. United States, 389 U.S. 347 (1967).

[72] United States v. Mandehall, 446 U.S. 544 (1980).

[73] Florida v. Royer, 460 U.S. 491 (1982).

[74] Griswold v. Connecticut, 381 U.S. 479 (1965), *Roe v. Wade*, 410 U.S. 113 (1973), and Whalen v. Roe, 429 U.S. 589 (1977).

[75] California Constitution art I, 1.

[76] The Privacy Act of 1974 (k), codified at 5 USC s 552a.

[77] FISA, 50 USC 1801.

[78] TIA is a program that intends to scan ultra-large databases of personal information to detect the information of terrorists. And CAPPS-II aims to conduct background risk assessments on all air travelers before they are get into commercial airliners.

[79] Tomko, G. Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy [online] <http://www.dss.state.ct.us/digital/tomko.htm>.

[80] McCormack, above n 18, 152-153.

[81] S.B. 169, 2001 Leg., 2001-2002 Session (Ca. 2001), 1798.87.

[82] Wong Kien K and Chia, K., 2001. E-com Legal Guide, Singapore.

[83] Computer Misuse Act, Ch 50A.

[84] U.S. DOS, Country Reports on Human Rights: Practices for 1996: Singapore [online] <http://www.privacy.org/pi/reports/hr96_privacy_report.html>.

[85] Gomez, J. and Smith, A., 2003. September 11 and Political Freedom: Asian Perspectives in James Gomez and Alan Smith (Ed.), September 11 and Political Freedom: Asian Perspectives xiii- xiii.

[86] Kennedy, D.C. In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty, *Richmond Journal of Law & Technology* 9 [online] <http://law.richmond.edu/jolt/v9i1/article3.html>.

[87] Lee Kwan Yew's Speech at National Day Rally, The Straits Times, April 20, 1987.

[88] Australian Broadcasting Corporation v. Lanah Game Meats Pty Ltd, 2001, 185 ALR 1.

[89] Electronic Privacy Information Center, Privacy and human rights 2003: an international survey of privacy laws and developments [online] <http://www.privacyinternational.org/survey/phr2003/countries/australia.htm>.

[90] Lyon, D. 2003. Surveillance after September 11, 81.

[91] New South Wales Law Reform Commission, above n 32, 39.

[92] Dripps, D.A., 2003. Reflections on the Criminal Justice System after September 11, 2001: Terror and Tolerance: Criminal Justice for the New Age of Anxiety, *The Ohio State Journal of Criminal Law* 9, 24.

[93] Crompton, M. Biometrics and Privacy: The End of The World as We Know It or The White Knight of Privacy? (Paper presented at the Biometrics Institute Conference, 20 March 2002) [online] <http://80-www.privacy.gov.au.exproxy.uow.edu.au:2048/news/speeches/sp80notes.htm>.

[94] Szyliowicz, above n 48.