A Comparison of Australian and Malaysian Views on the Use of Biometric Devices in Everyday Situations

Niranjala Weerakkody, Deakin University, Australia

Abstract: Since the September 11, 2001 terrorist attacks in New York City, many countries including Australia and Malaysia have been able to justify the use of biometric devices such as fingerprint scans, retinal scans and facial recognition for identification and surveillance of its citizens and others in the name of national security. In addition, biometric devices are increasingly being used worldwide by organizations to keep track of their employees and their productivity, leading to concerns of privacy, the safety, reliability, abuse and misuse of the data collected and violations of civil liberties. Taking the critical theory perspective, this paper will analyze the data collected and report on the findings of a survey carried out in Australia and Malaysia, with respect to the responses provided and opinions expressed to the survey's open ended and other questions by individuals as to their current use, experiences, preferences, concerns about the devices and the situations in which they think biometric devices should be used, including in their workplaces. This descriptive study uses both quantitative and qualitative data to examine what Australians and Malaysians think about the use of biometric devices in everyday situations and compare them as to their similarities and differences. The paper will then critically examine the ethical and civil liberties issues involved in the use of biometric devices in everyday life and argues that regulatory and legal measures should be taken to safeguard the rights of citizens while maintaining national security and productivity, in order to avoid the situation of Michel Foucault's Panopticon becoming an unpleasant everyday reality, which could negatively influence social justice and create social change due to its effects on individuals in two multicultural societies. The paper will argue about the need to educate the general public as to the issues of surveillance and privacy involved in the use of biometric devices in everyday situations.

Keywords: Biometric Devices, Biometric Identifiers, Electronic Surveillance, New Technologies and Privacy, Australia, Malaysia.

Introduction

In July 2004, 'The Age' newspaper published in Melbourne, Australia, reported an ethical and privacy violation involving the data collected via the practice of obtaining blood samples of newborns in hospitals in the state of Victoria in Australia since 1965 and all babies born in the state since 1970 (Noble, 2004). It reported that the organization in charge of the database had changed ownership several times over that period and the database with information on about 2 million subjects, was now held by a not-for-profit company with an active commercial focus, resulting in the data not being under the control of the state parliament. The information stored in this database could be obtained by police with a court order and the cards carrying the blood samples and other information of 1000 individuals from this database have already been given to researchers without any consent sought or obtained for making the data available to others or with the knowledge of the parents of the children or the individuals concerned.

The blood samples are collected as a means of testing for congenital disorders and are required to be held until the child turns two years of age, at which stage, the parents of the child are entitled to ask for the card as it is no longer required for the medical purposes they were intended for. However, very few parents of these babies or the adult individuals whose information is stored in the database, are aware of this right, know where these cards may be stored or who they should ask, if or when they want to get the cards back. The newspaper reported that the Victorian State government authorities were in the process of enacting legislation to safeguard this database from future abuses or misuses that could violate the principles of informed consent, voluntary participation (in later research using the data), privacy and civil liberties of the subjects that could cause them harm, according to standard ethical guidelines related to scientific research (Baxter & Babbie, 2004).

Rationale for Study

The above phenomenon known as 'function creep' (Economist, 2000) where data collected for one purpose is used for another without those who provided the data being aware of it, indicates the need for legal and other safeguards to be in place to protect databases carrying information on humans from being misused and abused, and thereby leading...
to violations of individual rights to privacy and civil liberties at a later time in unexpected ways. This need has become more urgent since the increased use of biometrics as identifiers of individuals by governments worldwide, in the name of national security and international terrorism prevention since the September 11, 2001 attacks in New York City, with little public debate or scrutiny and adequate legal safeguards or guidelines. Therefore, it is important to educate the public as to what biometrics are, what they can be used for, both the positives and the negatives of biometric technologies and the need for legal and other safeguards to guarantee the security of these databases and their potential abuses and misuses. This would help ensure citizens are adequately informed when allowing their governments to impose the compulsory use of biometric technologies in their everyday life.

**Biometric Devices**

According to the Association for Biometrics (UK), "biometric devices are used for the automated identification or verification of human identity through the measurement of repeatable physiological and behavioural characteristics" (cited in Kochan, 2004; 125). The most commonly used biometrics (to measure characteristics of a living thing) in identity verification instead of passwords, that are based on a person's physiological characteristics are facial features, the vein pattern in the retina via retina scans, iris scans, finger prints, hand shape, palm prints, and the vein patterns on hands. Behavioural biometrics that can be similarly used are handwriting (eg. signatures), voice analysis, signature dynamics, movement gait and keyboard typing rhythms (Smith, 2003; Lockie, 2002; Moody, 2004). Since the September 11, 2001 events, many nations including Australia, Malaysia and the USA, have drastically increased the use of biometrics for identity verification (to check if a person is who s/he says s/he is) and surveillance of their citizens and others for purposes of national security (Weerakkody, 2004; Kristoff, 2004; Clarke, 2001; van der Plogg, 2003).

**Advantages of Using Biometric Devices**

Mark Lockie (2002) traces the history of using biometrics for identity verification to 2600 BC where ancient Egyptians used body measurements to identify workers building the Great Pyramids (p. 58).

In 1960, the first true biometric system was developed and released by the Miller Brothers in New Jersey, USA in the form of a mechanical device that automatically measured the length of people's fingers (Lockie, 2002; 59). Over time, the costs related to biometric devices have been reduced making them more affordable to be used in everyday situations.

Swipe cards or Personal Identification Numbers (PIN) require a person to 'own' or 'know' something (Lockie, 2002), which can be easily left behind or forgotten. Many IT help desk calls are about forgotten passwords or PINS, which cost an organisation between $50-100 each (Moody, 2004). In contrast, a biometric is something a person 'is' such as a finger scan (Lockie, 2002; 11). They are most useful for providing restricted access to authorised individuals working in high security areas and for protecting confidential records or databases - such as in hospitals, from unauthorized access. They have also been useful in crime detection where 19 wanted criminals were identified with face scans at a stadium in Tampa, Fl. during the Super Bowl in 2001. The Sydney Olympics in 2000 had some parts of the athletes' village secured with biometric identifiers required for access (Lockie, 2002).

As biometric characteristics are unique to an individual, they can be assumed as highly reliable. Some biometrics can be used to differentiate between identical twins while some do not change across time for the same person. Biometric devices are more efficient and convenient to use in comparison to other methods of identity verification.

**Disadvantages of Biometrics**

The main disadvantage of biometric technology is that 4-10% of the population will not be able to provide a given biometric. Eg. The blind for iris scans or those without hands for finger prints. Finger prints can also be harder to read in females, Asians and manual workers. If a biometric record of a person is intercepted while being passed through a network or stolen from a smart card, unlike passwords or PINS, a new one cannot be issued. With the current level of vulnerability of networked security systems related to web browsers, servers and operating systems (Noguchi, 2004), and the use of traditional methods of forgery such as using Silicon films to forge finger prints, biometrics have proven to be fallible, contrary to popular beliefs and official claims (Economist, 2000). There is also a well known case of the Oregon man (who had recently converted to Islam), who was wrongly arrested on suspicion for the Madrid bombings in 2004, which indicates that the system is not fool proof. A person falsely accused of a crime based on biometric evidence, will find it hard to prove their innocence, as they are generally perceived as infallible.

The strongest argument against the use of biometrics is that they can be misused and abused by law enforcement and state authorities to keep citizens and others such as refugees, illegal immigrants and other marginalised or 'suspect' groups and individuals under surveillance and oppression, which can
lead to violations of privacy and civil liberties (Economist, 2000).

**Current Use of Biometrics in Australia**

All new passports issued in Australia since July 2004, carry a computer chip with the holder’s facial image. These ePassports are a result of the US government’s requirement that citizens of countries with Visa waiver status to visit the USA (for a period less than 90 days) to be issued only biometric passports after October 26, 2005. These ePassports will be used in conjunction with the SmartGate facial recognition technology currently being trialed at Sydney airport. The SmartGate will scan a person’s face and compare it with their ePassport photo and the gate will open for the person only if the two images match (Russell, 2004). Iris scans have been used for Qantas cabin crew on international flights at the Sydney airport, since long before the September 11, 2001 events.

The Australian Immigration Department plans to fingerprint suspected illegal immigrants (without consent if necessary) and give 28 days to confirm their identity (Hudson, 2005), before being sent for mandatory detention until their cases are heard. Even though touted as reducing the risk of illegal residents being wrongly arrested as illegal, as seen in the highly publicized case of Cornelia Rau— a former Qantas flight attendant and mentally ill permanent resident, who was wrongly held in detention for months, this measure allows the Australian government to provide information related to these illegal immigrants to other governments, particularly of those who fail in their visa applications to remain in Australia (SBS Online, 2003).

**Current Use of Biometrics in Malaysia**

Malaysia is the first country to issue biometric-enabled passports and currently several million of them are in use (Kochan, 2004). The Malaysian newspaper ‘Utusan Malaysia’ (2005) reports on a decision of the Malaysian Prime Minister Abdullah Ahmad Badawi to use biometrics for recruitment of Indonesian workers in Malaysia. Fingerprinting is to be introduced in a bid to combat the problem of 1 million Indonesian illegal immigrants in Malaysia, who come in search of work.

Malaysia also intends to issue all its citizens – teens and older, with a biometric ID card known as MyKad, that carries their fingerprint as a biometric in a computer chip. This card is to be used as a bank card, identity document, driver’s license, commuting pass, and will be later extended to voting and international travel (McGinty, 2005).

**Theoretical Framework**

This paper takes the critical perspective in examining the adoption of a new communication technology for both its advantages and disadvantages so that optimal uses can be made of it while keeping check of its abuses, misuses and negative effects. It will examine the potential of the technology and the data collected, to allow authorities and employers in democracies to keep their citizens, employees and others under surveillance which could adversely affect their civil liberties and privacy.

In the 1960s, the practice of computerized data collection and storage by state authorities and commercial organizations gave rise to fears of George Orwell’s ‘1984’ (Orwell, 1949) and ‘Big Brother’ governments (and corporations) keeping track of citizens, employees and consumers with analogies to Michel Foucault’s (1977) ‘Panopticism’ or ‘Panoptic surveillance’. Social theorists used the concept of the Panopticon with its ‘Wheel Configuration’ to ‘understand these emerging informational practices’ (Phillips, 2004: 695).

Biometrics support the accumulation and centralization of knowledge and information and ‘allow for individuals to be observed and acted upon as individuals, but understood as a collective’ with all knowledge concentrated with the central observer, who can then use this knowledge for creating ‘profiles’ of various groups. Based on these profiles, individuals and groups can be bestowed with punishments or gratifications based on how they fit the ‘norm’ set by the central observer (Foucault, 1977 cited in Phillips, 2004: 695). The political economy perspective sees this situation as serving the needs of capital (Gandy, 1993) such as when applied to organizations with employers keeping their employees under surveillance. This view is supported by the increasing use of biometrics and other technologies of surveillance by employers (Robinson, 2004) to keep track of work hours even of salaried workers to monitor their productivity (Maher, 2003 cited in Moody, 2004).

Hirschheim (1985) describes the three views related to the social impact of new technologies as optimistic (which takes an utopian view of technology being all positive and advocated by theorists such as Marshall McLuhan, 1969), pessimistic (where technologies are seen as increasing the power and control of those in authority as discussed in Bittker, 1986), which can lead to abuses and misuses, and pluralist (where technologies can be seen as neutral per se but how they are used depends on the desires and wishes of the designers and controllers of the technology and lead to either positive or negative outcomes based on their use (Burns, 1981). This paper takes the pluralist view of technology.
Literature Review

Biometric devices can automatically verify a person’s identity based on their unique physiological or behavioural characteristics, by comparing the characteristic with those of others in a database to find a match (Lockie 2002). In spite of being useful in forensic examinations to verify the identity of a person by matching samples, DNA, even though unique to each person, is not a biometric, as it is not yet fully automated.

Biometrics can give rise to two types of errors—namely false acceptance (accepting an imposter) and false reject (refusing a genuine person). It is also harder for biometrics to ‘identify a person’ (answer the question ‘Who is this?’) and is generally more suited for verifying a person’s identity (Lockie, 2002).

Yuki Noguchi (2004) describes how easy it is for anyone using Google searches to obtain many types of information such as lists of suspected Taliban or Al-Qaeda members and their details, access random medical records, bank account numbers, student grades, docking records of US Navy ships, submarines and destroyers etc. legally, by simply using the powerful search engine, due to many businesses and government agencies using it to transmit and store information. This raises concerns about the safety and confidentiality of any databases of information obtained as biometrics by governments and corporations worldwide, if each of the servers where this information is stored is linked to the Internet. The factors responsible for the ease in which outsiders can access such confidential information is due to improperly configured servers, weaknesses in the security systems and human error, which can make such information accessible to those not meant to have that access. Once Google or another search engine locates such information or databases, it is almost impossible to reverse the process.

Irma van der Plogg (2003) discusses how the increased surveillance needs of society have led to the spread of biometrics as a security solution. She points out that the two opposing lines of argument for their use are whether they are a threat to privacy or not. She examines the deterministic and voluntarist constructions of the technology as rhetorical devices and as discursive strategies which serve their own purposes in the political process of shaping biometric technologies. This argument can be illustrated by British Prime Minister Tony Blair’s introduction of fingerprinting as a requirement for all visa applications for the United Kingdom as a practical and systematic response to problems related to asylum and illegal immigration. However, the opposition Conservative Party had described this measure as ‘headline grabbing in time for the May (2005) election (SBS World News, 2005). Malaysian Prime Minister Ahmad Badawi’s decision to fingerprint illegal immigrants from Indonesia (Utusan Malaysia, 2005) too can be seen as politically motivated within the context of Malaysians’ increasing fears of and concerns about rising crime rates in the country, perceived as caused by these immigrants.

The US government’s passing of the Enhanced Border Security and Visa Entry Reform Act of 2002, which requires everyone entering the US after Oct. 26, 2004 (later extended to Oct. 26, 2005) to have biometric identification on travel documents (Grossman, 2003), has resulted in many other countries being compelled to adopt the technology, supporting the pessimistic view of technology that a technology can increase the power and authority of powerful nations and of all governments over their citizens and others. It also supports van der Plogg’s (2003) argument that certain purposes in the political process can shape biometric technologies.

David (2004) argues that biometric ID systems can only work with improved intelligence related to international terrorism. He sees the need for an improved profiling system, improved ‘no fly’ and ‘automatic selectee’ lists and improved sharing of information between various intelligence agencies (worldwide). The technologies used in different countries should also be interoperable or compatible with each other to use, if the new biometric passports etc are to be effective.

Kochan (2004) points out that for a successful application of biometric technology, it is necessary to use the correct biometric for each purpose as the various biometrics have both strengths and weaknesses. A fall back process is needed to accommodate those who cannot provide a given biometric such as the blinds’ inability to provide an iris scan. The support of the users of a given biometric and its implementation is also necessary, in order to avoid sabotage, and the improper or inaccurate use of the technology. In addition, the technology should be convenient to use and be secured against identity theft, aspects that are important to users of the systems.

Addressing the pessimistic view, Wadman (1999) sees how privacy advocates fear biometric systems can be abused by government and industry. Industry or an authoritarian state could use biometrics as an all purpose identifier (as proposed in Malaysia) that could be then used to ‘deny benefits, restrict travel or even obliterate the individual as a state-recognised entity’ (www.nature.com). Biometrics can identify a person in one area, which can then be used to adversely affect that person in another area such as for social security, police etc. (Simon Davis – Director, Privacy International cited in Wadman, 1999).

However, the International Biometric Industry Association (IBIA) argues that the technology is safe,
user-friendly and near perfect in terms of protection against identity theft and privacy abuses (Wadman, 1999). John Siedlarz – the Vice Chairman of IBIA and Vice President and Chief Executive Officer of New Jersey–based Iriscan considers biometrics as a tool for protecting privacy as it is more secure than PINs or passwords for computers and thereby enhanced in data security as only those authorised can access confidential records (Cited in Wadman, 1999). The IBIA believes that biometric data must not be released without personal consent or authority of law (Wadman, 1999). How data is collected, stored, accessed and used should be based on clearly defined policies and the data distribution should be reserved for their original purpose. How government agencies can acquire and use biometric data should be according to ‘clear legal standards’. Both private and public sectors should adopt suitable managerial and technical controls to protect databases containing biometrics (Wadman, 1999). The Economist (2000) cites the IBIA policy that insists governments’ use of biometrics to be strictly regulated and that transparency should be required of private companies that use biometrics. However, the Patriot Act implemented after September 11, 2001 in the USA, has completely overshadowed any other concerns on issues of privacy and surveillance related to biometrics or any other measures, as national security and border control and their corresponding discourses have dominated over civil liberties and individual rights. It has also changed biometrics from a niche technology to that of an ubiquitous one, within the space of a few years.

Methodology
This study used surveys returned by 230 individuals in Australia and 408 individuals in Malaysia, who were a part of a convenience sample selected via the researchers’ personal contacts and their acquaintances. The survey asked people what they think of the use of biometric devices in everyday life such as at Automatic Teller Machines (ATMs), logging into Personal Computers, buying products online, in schools to protect children, tracking employee work hours, security related to air travel, use by doctors and hospitals to guard patient records and maintaining security at stadiums and other public places.

It also asked respondents what they think about biometric devices and their efficiency (eg. Fast and more convenient; use of finger prints as sanitary) and collected their responses on a 5-point Likert scale (Baxter & Babbie, 2004; 170) that ranged from ‘strongly agree’ to ‘strongly disagree’.

The survey also examined the respondents’ preferences for using various biometric devices such as finger print scans, iris scans, retina scans, voice recognition and handwriting recognition when logging onto their computers, using the ATM or cashing a check, and gaining access to their offices. It then asked them what biometric devices of the aforementioned five preferences, would make them feel uncomfortable or reluctant to use.

However, this paper reports only on the open-ended questions posed in the survey about how the respondents currently use biometric devices, what their concerns about them are, and in what situations they think it is acceptable to use them.

The demographic details of the respondents as to their age group (10-20 years, 21-30, 31-50, 51+), sex, and level of education (some high school, completed high school, some university or technical college, university degree, and post graduate) were also collected.

Efforts were made to select respondents to fit a stratified sample of the population (eg. 50% of total respondents to be male and 50% female and 25% each to come from each of the four age groups listed in the survey etc.) (Baxter & Babbie, 2004). Based on this breakdown, the author used convenience samples of suitable individuals within these groups drawing on respondents from those among and with the help of one’s acquaintances in Australia. The Malaysian data was collected by an associate of the author in Malaysia from those among and with the help of the associate’s acquaintances, using the same guidelines whenever possible.

Findings
The survey responses were coded and examined using the Statistical package for the Social Sciences (SPSS 12.0) to provide a descriptive analysis of the data collected from the three open ended questions in the survey to discuss what the respondents knew about their current use of biometric devices in everyday life; their concerns about such devices and what they think how biometric devices should be used. The responses to the open ended questions were coded under various themes that evolved from the responses themselves and were labelled to illustrate the main arguments embedded in each theme. A preliminary data analysis of 75 surveys from Australia, were examined in Weerakkody (2004). Some of the discussions and conclusions made from that analysis were found to be applicable to this comparative analysis as well and have been included in this paper.

Current use of Biometric Devices
In the Australian sample, 45.1% or 103 of 230 respondents and in the Malaysian sample 44.8% or 184 of 408 respondents did not respond to this question. Of those who did, 77.1% or 98 in Australia
and 56.25% or 126 in Malaysia reported that they currently did not use them. For Australian respondents who answered this question, the most used biometric was handwriting for banking (4 or 3.1%), for passports (3 or 2.3%), voice for mobile phone, for ID purposes, and at airports (2 or 1.5%). For those Malaysians who responded to this question, the most used was handwriting for banking (40 or 17.85%), for ID purposes (16 or 7.1%), and passports (4 or 1.8%).

Concerns about Biometric Devices

The 'no response' rates for this question for Australia were 56 or 24.3% and for Malaysia, it was 135 or 33.1%. Of those responded, 22 or 12.6% in Australia and 22 or 6.9% in Malaysia indicated that they were not concerned about the use of biometrics. However, 48 respondents or 17.6% in Malaysia indicated they support the use of biometrics while no Australians respondents did so.

For Australian respondents who answered the question, the main categories of concerns were Invasion of privacy (35 or 20.1%); Reliability of the technology (i.e., system breakdowns) (16 or 9.2%); Physical side effects to the body and surveillance (13 or 7.5% each); misuse/abuse of data collected (11 or 6.3%); and inconvenience (10 or 5.7%). For Malaysians who responded, the top categories were misuse/abuse of data (25 or 9.15%); Safety (positively involved in using biometrics) (23 or 8.4%); Reliability of the technology- again positively (21 or 7.7%); negative physical side effects (18 or 6.6%); Invasion of privacy (16 or 5.9%); and hygiene issues (1 or 0.3%).

Two (or 1.1%) of the Australians who responded indicated civil liberties as a concern while no one indicated the technology as increasing safety. Among the Malaysians, only 2 (or 0.73%) indicated surveillance as a concern and no one mentioned civil liberties.

A few respondents in both countries feared being forced by criminals to provide their biometric identifications to access restricted areas by cutting fingers or eyes for the purpose etc. (They may have learnt this from movies such as 'Demolition Man' and internalized it without attributing it to the media). A few actually mentioned movies such as 'Gattaca' (1997), 'Minority Report' (2002) and 'Charlie's Angels' (2000 & 2003), without providing a specific context to their comments.

Reliability / Accuracy/Efficiency / Inconvenience Involved in Using Biometrics

Some respondents were concerned about the costs of the systems, which could be passed on to the public; glitches of the systems; the systems being too complicated; having room for error; time consuming; and questioned if biometrics would be any more effective than other technologies used for identity verification.

Pessimistic Views of Technology

Under this category, respondents expressed fears of government controls; violation of civil liberties; being used for monitoring of staff instead of for security; creating a culture of fear; mistrust and authoritarian control; leading to excessive use, paranoia and '1984'; used in situations where it is not needed; taking biology as a means of truth; leading to global conspiracy; and that they may be socially unnecessary.

Practical Concerns

Some respondents thought biometric devices will be unnecessarily restrictive where one can't lend one's bank card to their partner or log on to others' computers and that they may inhibit freedom of movement.

Exclusion of Some Individuals

Six Malaysians and two Australians were concerned about those who may be unable to provide a biometric for identification such as due to amputations, having fingers in casts etc.

When Should Biometric Devices be Used

Among those surveyed, 37.0% or 85 in Australia and 107 or 26.2% in Malaysia did not answer this question. Of those who did, the main uses suggested by Australians were for security without infringing on personal liberties (23 or 15.9%); Banking and related activities (20 or 13.8%); Air travel (17 or 11.7%); in high security situations (15 or 10.3%); and for accessing personal records (11 or 7.6).

For the Malaysians respondents, the highest ranked uses suggested were Banking/credit card and related activities (77 or 25.6%); for security without impinging on personal liberties (69 or 22.9%); to protect personal records (28 or 9.3%); to improve public safety (14 or 4.7%); detect crime (12 or 4.0%); and in high security situations (9 or 3.0%).

A few Australian respondents stated that 'we should not use them, don't need them, they need to be investigated more' or questioned if they are 'any better than other methods', while no Malaysian respondents indicated same.
Discussion

Many respondents had indicated to the researcher and to her associates who helped distribute the surveys that they had not known what biometric devices were until they read the definition in the survey even though a good percentage of the respondents were higher educated. Many also had not provided responses to the open ended questions.

Australians are well known for traveling overseas and will be faced with biometrics at airports and in their passports. Malaysians already use them in larger numbers and had been for some time. They are also very likely to be issued with the MyKad in the foreseeable future (McGinity, 2005), which will be used for multiple purposes and linked to several databases, making it easy for surveillance and access by many institutions. Once biometrics become widely used, it will be hard to refuse to or not be part of them. Biometric devices are seen as tools that can limit our freedoms and repress 'different thinkers', public interest advocates and other 'trouble makers' and dissenters (Clarke, 2001). Their use has the potential to create a situation where 'technological imperatives' will override those of democracy (Safire, 2004).

In modern times, they can be a necessary evil as the 'right to life' (from terrorism) will be more important than possible violations of individual privacy, civil liberties and freedoms, as already experienced with the US Patriot Act. However, as William Safire (2004) argues, the right to stay alive, needs to be balanced with the right to be left alone post September 11.

The findings show that even if most respondents see the positives as well as negatives of biometric devices and their potential to violate privacy, for abuse and misuse of data, be harmful to their health or body and be unreliable and inconvenient to use, no one appears to indicate that legal safeguards should be in place to protect individual rights, in the open ended questions which asks them how biometrics should be used. In such an environment, it will be very easy for authorities in Australia or elsewhere to pass laws or introduce procedures regarding biometric devices that will violate civil liberties and individual privacy, without any accompanying legal or administrative safeguards and guidelines.

Australia has a record of law enforcement organizations using phone taps as the easy way out for crime detection, resulting in misuse of powers and violating the rights of innocent third parties, who also fall under surveillance in the process. On several occasions, unauthorized access to databases to obtain negative information on certain individuals- such as political candidates, by individual police officers during election campaigns have been reported in the state of Victoria. In August 2005, a female resident of Victoria had reported to the Ombudsman of being threatened by a local female police officer in her town that the police officer would access information on her husband from the police database in order to discredit him. The woman requested that her husband's files be checked to see if any unauthorized access to their files had been made. After checking the database for the information requested, the Office of Police Integrity had sent her two folders of confidential police files detailing that her husband's file had been accessed in April 2004 generating 10 pages of computer print outs. However, in the same package they had inadvertently included details of 450 other individuals including details of criminal offenders and victims. This matter is currently under investigation (Austin, 2005). These indicate the current level of poor security related to police databases and their abuses and misuses.

Conclusion

There appear to be some differences between the themes and categories of responses given by respondents in the two countries, which may be due to their different cultural, social and political systems and realities, which need further study. The use of convenient samples for the survey also limits the generalisability of the findings. However, this preliminary survey serves as a pilot study for further research on the subject (Baxter & Babbie, 2004). Any further research could include interviews with members of the public who do, as well as who do not have experience with using biometric devices; vendors of the technology; policy makers and government officials in charge of implementing the technology and related policies; privacy advocates; and technical specialists of biometric technologies. These interviews can be supplemented with focus groups with citizens to garner their views on biometrics for comparison with those of experts, vendors, policy makers, and law enforcement and government officials.

Such a research design will be utilizing the strategy of methodological triangulation (Baxter & Babbie, 2004).

As for the case in Australia, specific regulations are needed to safeguard individuals' rights when biometric devices are used in everyday situations. They should be related to the storage of biometric measures, design standards for measuring devices, prohibitions related to the manufacture, import, installation and use of biometric devices, audits of compliance of devices and ethical guidelines (Phillips, 2004) to safeguard the rights of individuals and protect the data gathered about and from individuals. EPIC (2004) lists the areas that need to be addressed in policy making as storage, vulnerability (of data), confidence (acceptable error rate), authenticity (can information be tampered with), linking (limits on
private vs government use, and ubiquity (implications of having an electronic trail on individuals when commonly used with other technologies of surveillance).

The general public in Australia need to be educated about this 'mixed blessing' so that they will expect the government and law enforcement authorities to be more accountable regarding the methods and situations in which data are collected, stored and disseminated and that civil liberties are not sacrificed in the name of national security or administrative efficiency.

As the Justification Model of Technology (Hamelink, 1988) suggests, the implementation of a new technology is a 'social gamble' as we do not know everything about it, its capabilities or how it may be used once adopted by society. E.g. No one foresaw the Internet being used by under age kids to download pornography. As the pluralist view suggests, the technology may be neutral or even useful per se but its implementation needs to be balanced between the wishes of the implementers and the rights of those who are affected by the implementation.

Some respondents had suggested the devices should be used only in extremely sensitive situations such as the military, defense, air travel etc and only to supplement non-biometric methods. There should also be checks and balances to secure these data from abuses and only be allowed access by those who need to do so under specific conditions. Even though technological determinists may argue that technology is its own driving force, one should not forget the role of society and its power holders in deciding how it is to be used and for what purposes (van der Ploeg, 2003). As biometric technologies are still new, we also need to learn more about them before their widespread application, currently based on their perceived accuracy and infallibility, which should be subjected to further examination.

References


**Note:** This paper is part of a larger study examining public opinion on biometric devices in Australia, Malaysia and the USA. The study and its survey instrument were designed by Associate Professor Janette Moody of The Citadel (University), Charleston, SC, USA, while the author served as co-investigator. The author wishes to thank Dr. Jamilah Ahmad of University Science Malaysia (USM), Penang, for collecting the Malaysian data and Ms Jo Gulli of the Corporate Citizenship Research Unit (CCRU) at Deakin University, for the valuable research assistance provided.

---

**About the Author**

*Dr. Niranjala Weerakkody*

Niranjala Weerakkody, Ph D, Rutegera, U, NJ, USA is a Senior Lecturer in Media and Communication in the School of Communication and Creative Arts at Deakin University.