A Preliminary Examination of Public Opinion in Australia on the Use of Biometric Devices or Identifiers in Everyday Life.

Niranjala D Weerakkody PhD
School of Communication & Creative Arts, Deakin University
Geelong VIC 3217, Australia

ABSTRACT

Since the September 11, 2001 terrorist attacks in New York City, many countries including Australia have been able to justify the use of biometric devices for identification and surveillance of their own citizens and others in the name of national security.

This paper reports on the preliminary findings of a survey that examined Australians’ views and experiences with the use of biometric devices in everyday situations in the context of their potential to serve as a ‘Panopticon’ to keep the nation’s citizenry under surveillance. It discusses the adoption of the new communication technology from the point of view of the Justification model that sees technology choice as social gambling and the pluralist view of technology that sees technology as neutral in itself but as having negative or positive effects on society based on how it is used.

The paper proposes the need for Australian society to balance citizens’ right to privacy and civil liberties with the right to stay alive and safe from terrorism and how it may be done with the necessary legal and regulatory safeguards.

Keywords: Biometric Devices, Biometric Identifiers, Surveillance Societies, Adoption of a New Communication Technology in Australia, Biometric Devices and Privacy, Surveillance Technologies

INTRODUCTION

Biometric devices or identifiers are electronic devices that measure some aspect of an individual’s physical uniqueness and are used to verify a person’s identification instead of using passwords or PINs (Personal Identification Numbers). The most popular biometric devices used today are fingerprint scans, hand geometry, retina scans, iris scans, facial recognition, voice recognition and handwriting recognition (Singleton, 2003).

Beginning January 5, 2004 and as phase one of US-VISIT, a US$380 million effort to track terrorists, immigration officials at all international airports in the USA have vetted visitor passports and visas and posed security questions before taking fingerprints and photographs of arrivals. Within three days of its implementation, US-VISIT was operating at 115 airports photographing 83,000 international passengers and nabbing 30 suspected criminals (AFP, 2004b). By 2005, every US port of entry on land, sea and air will be equipped with finger printing and photographic technology for the purpose. All US visas and passports will eventually include photographs and fingerprints (AFP, 2004a). This AFP (2004 b) news item further reported that based on the ‘principal of reciprocity’, the Brazilian police started fingerprinting and photographing Americans arriving in their country at Sao Paulo airport, beginning January 1, 2004, under a judicial decision of their federal court and leading to long delays for passengers going through the procedure (Rohter, 2004b).

In addition to national security, biometric identifiers are increasingly being used by organizations to keep track of its employees and their productivity, leading to concerns of privacy and civil rights violations (Maher, 2003).

RATIONALE FOR THE STUDY

This paper is based on the premise that organizations and governments are requiring increased accountability and surveillance of their employees and citizens and use biometrics as one way of accomplishing that end (Worthen, 2002). The Wall Street Journal of 4th November 2003 noted that employers are increasingly using biometrics to monitor not just their hourly employees but also their salaried staff, which had led to protests from workplace rights advocates (Maher, 2003).

Since September 11, 2001 terrorist attacks on the New York World Trade Center Twin Towers, authorities in many countries have been able to justify the use various methods of biometric scans of identifications and surveillance of citizens and others, to monitor individuals and their activities in the name of national security and border protection. For example, Qantas airlines of Australia already uses iris scans for identification of and access to its cabin crews, while within the next 10 years, Britain is planning to introduce passports and driving licenses with biometric data such as eye recognition and fingerprints in databases. It is suggested as a means of fighting social security fraud, immigration abuse and terrorism (ABC Online, 2003).
Since September 11, 2001, most Islamic individuals living in or visiting many Western democratic nations including Australia have complained about having their civil liberties and individual freedoms violated and suspected of involvement in terrorism, based on the principle of demographic and criminal profiling (EPIC, 2003). The use of biometric devices has potential to further increase their marginalization, discrimination and harassment.

Therefore, it is timely and important to examine the issue of the use of biometric devices in a democratic nation such as Australia.

THEORETICAL FRAMEWORK

The use of biometric devices and other such surveillance technologies that are used to monitor the actions and behaviors of citizens and individuals increase the power of employers, law enforcement organizations and other authorities. They give rise to fears of Michel Foucault’s (1977) ‘Panopticon’ and of ‘Big Brother’ (Orwell, 1949). These fall under the pessimistic view of new communication technologies (Hirschheim, 1985), because such measures and policies could lead to widespread abuses of authority, information, and violations of privacy and civil liberties.

Biometric Devices as the ‘Panopticon’

Michel Foucault (1977) sees the power exercised on our bodies as

"...conceived not as a property, but as a strategy, that its effects of domination are attributed not to 'appropriation', but to dispossession, manoeuvres, tactics, techniques, functionings; that one should decipher it as a network of relations, constantly in tension, in activity, rather than a privilege that one might possess..." (p. 26).

New computerized technologies such as databases and surveillance systems can provide law enforcement agencies and employers the ability to keep individuals, their actions and behaviors under surveillance at all times. As a result, they could lead to people becoming ‘acclimated to order and obedience’ (Foucault, 1977, p. 215) due to the presence of Panopticon-like situations that can keep large numbers of people and groups under surveillance using few ‘observers’ (Foucault, 1977, p. 217). Newer data gathering, storage and disseminating methods and technologies such as biometric devices can become the circuits of communication that are already the ‘supports of an accumulation and centralization of knowledge’ (or information) about individuals (Foucault, 1977, p. 217). As a result, biometric devices give increased powers to the authorities and institutions of law enforcement and serve as a ‘Panopticon’. In the wrong hands or if misused, such surveillance measures, the administration and enforcement of such procedures, and the data gathered with these technologies, can lead to discrimination, inconveniences and harassment as reported in Brazil where overzealous customs officials fined and held overnight and American airline pilot for ‘disrespect for authority’ (Rohrer, 2004 a). The airline later apologized to the Brazilian authorities on behalf of its ‘offending’ employee.

The Justification Model of Technology

The Justification Model of Technology (Hamelink, 1988) sees the adoption of a new technology as a form of ‘social gambling’ as no one can accurately predict what a technology can do as we only have partial knowledge of its capabilities and uses. Once adopted, we also cannot predict or envisage how it will be used, for what or what its overall effects will be.

The Pluralist View of New Technology

Hirschheim (1985) describes the individual and social impact of new communication technologies under three broad positions—namely the optimistic, pessimistic and pluralist views. The optimistic view takes an utopian approach to new technologies seeing it as improving efficiency, productivity and communication and social equality (McLuhan, 1969). The opposing pessimistic view sees new communication technologies as helping to extend the power and control of those in power and authority (Beniger, 1986). The pluralist view sees new communication technologies as apolitical or neutral—such as a building block, but as a structure reflects the desires and wishes of the designers and controllers of the system (Burns, 1981). In other words, the pluralist view positions new communication technologies as creating possibilities, which will be either positive or negative, based on how they are used or implemented (Hirschheim, 1985).

This paper takes the pluralist view and examines the issues under the Justification Model of technology. It will argue that biometric devices have the capacity to serve as a ‘Panopticon’ and therefore it is necessary to make sure that their use does not function as a means of oppression and unlawful or unfair control of its individual citizens and marginalized groups.

LITERATURE REVIEW

In his paper ‘Biometrics and privacy’, Clarke (2001) argues that:

Biometric technologies have extremely serious implications for human rights in general, and privacy in particular. Their uses to date have been to enable powerful organizations to exercise social control over people, and the designs have been highly insensitive to the interests of the individuals they are imposed upon.


Clarke (2001) also argues that biometric technology providers’ claim that they can provide ‘identity verification’ is a misleading exaggeration because they actually are referring to ‘identity authentication’ which gives the false impression of their method being foolproof and can deliver verity or ‘truth’. This is because authentication is simply an establishment of a degree of confidence about the truth of an assertion about a person’s identity (i.e. is he who he says he is?) where ‘organizations acquire information about a person in order to check it against previously recorded information. Hence, authentication is a process of one-to-one comparison, rather than a mass searching process’ (Clarke, 2001).


However, some biometric schemes can be devised to have substantial accuracy. But they are generally expensive, inconvenient, intrusive and limited to specific contexts. At the same time, they can be defeated (Clarke, 2001).
The Negative Aspects of Biometric Data Collection

The collection of biometric data from individuals can be demeaning (e.g., Being asked to provide body fluids or tissues), intrusive, disrespectful (e.g., Holding someone’s hand when fingerprinting), uncomfortable (e.g., Waiting in lines at airports for photographing) and inconvenient: They violate the privacy of the people being checked (Clarke, 2001). Once collected, the data will be shared between various organizations and institutions, which increases the control they have over individuals. They can also provide information about individuals’ behaviors to organizations. As biometric systems are expensive, organizations could share schemes such as cards for several purposes resulting in data sharing between organizations. Biometrics take away the ability of individuals to remain anonymous or use pseudonyms when carrying out commercial or other transactions due to data matching and cheaper methods of data storage. Imposters can fabricate or use biometric data of another individual. Identity theft occurs when such imposters carry out several masquerades or live permanently with the same stolen identity. As biometric devices are presented by their systems providers as ‘foolproof’, an affected party will find it very hard to prove their innocence. Unlike Personal Identification Numbers (PINs) or passwords used as other means of access and identification, biometric identifiers cannot be changed to keep them secure (Clarke, 2001).

Even though individuals may dislike the use of biometric identifiers, they will be unable or powerless to oppose their use by employers and authorities as seen with their use at US airports and in many other situations when national security superseded individual freedoms after September 11, 2001 (Kristoff, 2004). Biometric Devices and ‘Soft Targets’

Australia is in the process of passing new laws to force asylum seekers and refugees who have lost their identity documents to have their photos taken, have iris scans, have their finger prints and palm prints taken to prove their identity. Proposed as a means of countering identity fraud and to protect national security, the laws will enable the Australian government to provide that information to other governments, particularly in the case of people who fail in their visa applications to remain in Australia.

The opposition (Australian) Democrats party leader Andrew Bartlett fears these laws could be abused by guards at the controversial asylum-seeker detention centers in Australia to intimidate the already marginalized refugee detainees (SBS Radio News, 26/06/2003). Convergence

Until recently, the use of biometric devices within organizations and governments had been limited due to the bulkiness of the equipment and the related high costs of adopting the technology.

The adoption of biometric authentication systems also have been developed as stand alone or as ‘point’ solutions such as one department using a fingerprint reader to grant access to a personal computer, while another deploys hand-scanning technology in a secure area with no connectivity between the two technologies. As a result, biometric devices have typically existed as ‘islands’ without integration to centralized back-end systems and directories (Carr, 2001).

However, the fast decreasing cost of the technology and the convergence of the of disparate methods of biometric authentication into one integrated product has now allowed authorities and organizations to use a variety of biometric devices together with one back-end system, which allows connectivity between systems able to share directories and information (Carr, 2001). This allows authorities and organizations increased control of their citizens, staff, and others about their work, movements, activities and other personal information fitting with the concept of Foucault’s (1977) Panopticon. Even though this is an efficient and convenient system of maintaining security of a nation or organization and for collecting, storing and sharing data on a large number of individuals and locations, if misused, such back-end systems and directories can lead to violations of privacy and civil liberties of individuals and groups. This brings to mind the predictions and warnings of a ‘Big Brother’ as first popularised by George Orwell in his book ‘Nineteen Eight-Four’ (Orwell, 1949) and popular Hollywood movies such as ‘Gattaca’ (1997).

To examine how Australian’s perceive the use of biometric devices in Australia, a survey was conducted in early 2004. Based on the data collected from the survey, this paper reports on what individuals in Australia currently know and think about biometric devices in their everyday life situations as well as concerns about their potential uses and abuses.

METHODOLOGY

The project collected data from a preliminary sample of 75 respondents in Australia using a survey instrument that asked them what they think about the use of various biometric devices in various areas of their everyday life such as at Automatic Teller Machines (ATMs), logging into a personal computer, purchase of products on line, 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.

The survey asked what the respondents think of these biometric devices and their efficiency (e.g., faster and more convenient, use of fingerprint scans as unsanitary). Respondents provided their responses to these questions via a 5-point Likert scale (Baxter & Babbie, 2004, 170) that ranged from 'strongly agree' to 'strongly disagree'. It also examined the respondents' preferences of the various biometric devices such as fingerprint scans, iris scans, retina scans, voice recognition and handwriting recognition when logging on to their computers, using the ATM or cashing a
check, and gaining access to their offices. It then asked what biometric devices of the above-mentioned five preferences, would make them feel uncomfortable or reluctant to use.

However, this paper only reports on the comments made by respondents to the open-ended questions posed in the survey about how they currently use any biometric devices, what their concerns about biometric devices are and what they think of the situations in which biometric devices should be used.

The demographic details of the respondents collected were their age (10-20 years, 21-30, 31-50, 51+), level of education (some high school, completed high school, some university or technical college, university degree, and post graduate). Efforts were made to select respondents to fit a stratified sample of the population (e.g., 50% of total respondents to be male and 50% female; 25% each to come from the four age groups listed in the survey etc.) (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, as a preliminary examination of the issues under study.

FINDINGS

The survey responses were examined 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.

Sex of Respondents

Demographically, the 75 respondents who participated in this preliminary study via the survey consisted of 39 (52%) males and 36 (48%) females. One respondent (1.3%) did not provide a response to the question.

Age

The respondents’ distribution in terms of their age groups was 11 (14.7%) between the ages of 10 and 20 years, 22 (29.3%) in the group between 21 and 30 years, 24 (32%) in the 31-50 age group and 17 (22.6%) in the over 51 age group. One respondent (1.3%) had not answered this question.

Level of Education

Ten (13.3%) of the 75 respondents had reported having some high school education, six (8%) as high school graduates, 6 (8%) with some university study or trade certificate, 26 (34.7%) with university degrees and 25 (33.3%) with post graduate study. Two respondents (2.7%) had failed to provide an answer to this question.

The sample’s bias towards the higher educated can be explained as resulting from the author’s use of her colleagues at an academic institution and their acquaintances as respondents in a convenience sample for the survey.

However, since this study was using a convenience sample, this bias can be accepted. At the same time, the findings would indicate what some of the higher educated in Australia know and think about biometric devices.

Current Use of Biometric Devices

Of the 75 respondents who participated in the survey, 43 (56%) indicated they did not currently use any biometric devices while one reported using fingerprinting to log on at work and two indicated they used various forms of handwriting or signatures at the bank, while one thought she used voice recognition on her mobile phone. One did not know if she used them or not and 25 (33.3%) had not responded to the question.

An interesting finding from the data is that even though banks have been using or had the capability to check signatures of customers for some time, only two respondents recognized handwriting / signatures as an application of a biometric device.

Respondents’ Concerns about Biometric Devices

Twenty (26.7%) respondents failed to answer this question, but those who did, provided one or more responses to the question “My concerns about using biometric devices are”. The top four themes of responses to this question related to invasions of privacy (12 responses), health concerns (11), potential for abuse / misuse / forgery of the data (11) and the reliability / accuracy / efficiency of the systems dealing with biometric data (11).

The specific opinions expressed under these themes can be framed as: “Too much invasion / loss of privacy in private and public places”. Under health concerns, the specific responses were “Retina scans can be harmful to the eye; It is an invasion of the body; There will be side effects or body damage; and Fingerprint scans can be unhygienic”.

Under potential for misuse / abuse / forgery of the data, various respondents expressed fears that “They will be misused for consumer persuasion” (i.e. advertising); Concerns about “Who uses / abuses the data? Who keeps the data? Others could use my personal information; And there is potential for forgery” (by hackers etc.).

Two respondents also feared of being forced by criminals using violence against them, to provide their biometric identifications such as fingerprints, to access restricted areas. Fears of “Criminals cutting off fingers or eyes for the purpose” were also expressed. One feared for the security of the devices that store their biometric data.

With reference to the reliability / accuracy / efficiency of the systems dealing with biometric data, some respondents expressed the view that “the systems may be costly, which will then be passed on to the public”. Others feared lack of accuracy, reliability and “glitches in the system”; the systems as “too complicated”; There is “too much room for error”; that “hand writing / voices can be copied” (forged); and that the systems will be “time consuming” (for checking of individuals). One asked if these biometric systems were “any more secure than other systems”.

The opinions falling under the pessimistic view of technology included those related to control by authorities / employers (6 respondents). They included “fears of government control”; “violation of civil liberties”; “instead of for security, it will be used for the monitoring of staff”; “It creates a culture of fear and authority”; It will “lead to excessive paranoia” and “1984”. It will be “used in many situations which don’t need them”; “It will change the focus of society on biology as a means of truth”; It will lead to an “over the top use”; That “it (biometrics) will become a requirement to low level security situations”, it may
"lead to government control" or "global conspiracy". Some respondents thought biometric devices symbolized "too much concern about security" or an "unnecessary degree of security" and that they are "socially unnecessary".

In a more practical sense, one respondent thought biometric devices could be "unnecessarily restrictive" as one "cannot lend (one's) bank card to (one's) partner or log on to other computers". Another thought they "inhibit freedom of movement".

At the same time, there were six respondents (8%) who were "not concerned" about the use of biometric devices in everyday life.

Respondents' Views on when Biometric Devices should be used

Twenty-six (34.7%) of the 75 respondents of the survey did not answer this question. However, of those who did 25 (or 33.3% of total) thought that biometric devices should be used in high security contexts such as in military/army or other defense forces, air ports, immigration, for increased security of the airways or other high security situations. The next largest group wanted them at ATMs banking (9 respondents or 12% of total), for other banking purposes such as accessing their accounts, for Internet banking and to enter bank buildings (5 or 5.3%). But, one respondent (1.3%) preferred passwords to biometric devices.

Using biometrics for 'identity verification' was proposed by five (6.7% of total) respondents. Six respondents (8%) wanted them for "protecting sensitive information", to access "confidential files", "computers" (4 or 5.3%) or "workplaces" (1 or 1.3%). One (1.3%) suggested that with data gathered via biometric devices, they should "only allow access to that information to relevant people".

With reference to law enforcement, only two (2.6%) respondents approved the use of biometrics for apprehending criminals and detecting frauds. Three respondents (4%) indicated they don’t "like it" or "agree with their use" while two (2.6%) thought, "They are not any better or more useful than other methods" or they "don’t make much difference to security or safety".

Two respondents (2.6%) indicated that they should be used "only when extremely necessary" and one (1.3%) thought their "uses need to be investigated more". One respondent (1.3%) did not agree with their use while two (2.6%) said there were no suitable situations for the use of biometric devices they could think of and two (2.6%) thought "we don’t need them".

Two (2.6%) respondents thought biometrics should not be used for "monitoring actions or work". But it was interesting to note that one respondent (1.3%) proposed biometrics "to track employee hours" as one of the ways they should be used.

In general, the data indicates that respondents who expressed their views were cautious and concerned about the use of biometric devices in everyday situations.

**DISCUSSION**

Anecdotal evidence suggests that a good number of the respondents to the survey did not know what the term 'biometric devices' meant until they read the definition provided in the survey, despite the high percentage of higher educated individuals who made up the 75 respondents. The high number of 'no responses' to the three open ended questions also indicated that many of the respondents (which have to include at least some of the higher educated due to the lower numbers of those with lower educational qualifications), also had little or nothing to say about their use.

Australians are well known for their love of overseas travel and will face the use of biometrics in their passports in the near future (as new ones are already equipped with biometric identifiers) and when visiting other countries. Even though Australian nationals do not need a visa to visit the USA for business or pleasure for durations less than three months, they still have to undergo photographing and fingerprinting at US airports. It would be a matter of time when all Australian passports will include biometric identifications to meet the specifications of the USA imposed due to international terrorism.

Anyone refusing to subject themselves to biometric devices for identification can be seen as suspect as the general argument will be "Why should you be scared if you do not have anything to hide?" This discourse and its framing will eliminate the issues of democracy, privacy, civil liberties, personal freedoms and choices from the discussion. Clarke (2001) argues that biometric tools are among the most threatening of all surveillance technologies, agreeing with Foucault's (1977) views, because they have the ability to limit our freedoms. They can also repress 'different thinkers', public interest advocates and other so called 'trouble makers'. In the wake of the terrorist threats worldwide-especially in the western democracies such as Australia and the USA, 'technological imperatives' have overtaken democratic freedoms.

In modern times, therefore, biometric devices could be a necessary evil as the right to life (due to the threats of terrorism) will become more important than the right to individual privacy that can be violated with them. However, as William Safire (2004) argues, the 'right to stay alive' needs to be balanced with the 'right to be left alone' even though the passion had gone out of the advocacy for privacy and civil rights since the September 11 (2001) as seen with the adoption of biometric devices and the imposition of the Patriot Act in the USA, with little public debate or opposition.

The findings of the study on which the paper is based also indicate an interesting situation. Even though many respondents have understood the negative effects on privacy that arise with the use of biometric devices, and say access to the data collected should be limited or the systems may not be secure or even that it may be unnecessary to use biometric devices, none had mentioned any legal safeguards that should be available to protect their rights. A good number appear to be ignorant of the issues involved or unaware or indifferent to what is at stake when they do not respond to the open ended questions. In such an environment, governments will find it very easy to pass laws that limit our civil liberties in the name of national security, as done with other surveillance technologies such as telephone tapping and electronic eavesdropping devices in Australia in recent times. Many violations and misuses of powers occurred with those technologies as law enforcement organizations used wiretaps as an easy way out in crime detection, violating the
CONCLUSION

Clarke (2001) suggests specific regulatory measures that may be used to safeguard individual rights in an era where biometric devices will be used in everyday situations. These relate to the collection, storage, use, and dissemination of biometric data. If biometric devices and devices related to the manufacture, import, or export of biometric devices are to be used to protect the rights and security of individuals, the devices themselves must be subject to controls. At the same time, the protection of common law concepts and the development of national and international legal frameworks are needed to ensure that the use of biometric devices is regulated to ensure that privacy and civil liberties are not sacrificed for the sake of national security or administrative efficiency.

In other words, one must acknowledge that policy making about the adoption of a new technology is a gamble as suggested by the Justification Model (Hamelink, 1988). As the pluralist view suggests (Hirschhiem, 1985) biometric devices as a technology per se may be neutral, but its implementation will reflect the desires of those in a position to make decisions regarding it. Therefore, their desires need to be balanced with the interests and desires of those who will be affected by the implementation.

Some respondents have suggested that biometric devices should only be used in extremely sensitive situations such as military, defense, airways, etc. and only to supplement other non-biometric methods. There should also be checks and balances to secure these data from misuse and only allowed to be accessed by those who need to do so under specific conditions. In other words, protections, regulations, laws, and guidelines should be in place to guarantee biometric devices do not serve as a 'Panopticon' in a surveillance society (Foucault, 1977).

REFERENCES


Babbage, E 2004, The practice of social research, 10th edn., Wadsworth / Thomson Learning, Belmont, CA


Burtis, A 1981, The microchip: Appropriate or inappropriate technology? Ellis Harwood: Chichester


McLuhan, M 1969, Interview with Eric Norden: A candid conversation with the high priest of pop cult and metaphysician of media. Playboy, March, 53-62, 64-6, 68. 70, 72, 74. 148.


Worthing, B 2002, How to meet tomorrow’s privacy rules today. CIO. 19(3), 1-3

Note: The data collected in Australia on which this paper is based, were part of a larger study that examined public opinion of citizens on the use of biometric devices in the USA, Canada, Australia, Malaysia and Sri Lanka. The study and the survey instrument used were designed by the chief investigator of the project: Associate Professor Janette Moody of the Citadel, Charleston, NC, USA while the author served as co-investigator.