A Comparative Analysis of Opinions of Americans, Australians and Malaysians on the Use of Biometric Devices in Workplaces for Security and Monitoring of Worker Productivity

Niranjala Weerakkody, Deakin University, Australia

Abstract: Since the September 11, 2001 terrorist attacks in New York, the use of biometric devices such as fingerprint scans, retina and iris scans and facial recognition in everyday situations for national security and border control, have become commonplace. This has resulted in the biometric industry moving from being a niche technology to one that is ubiquitous. As a result, more and more employers are using biometrics to secure staff access to their facilities as well as for tracking work hours, maintaining 'discipline' and carry out surveillance against thefts, detecting work hour abuses and fraud. However, the data thus collected and the technologies themselves are feared of having the potential for and actually being misused – both in terms of the violating staff privacy and discrimination and oppression of targeted workers. This paper examines the issue of using biometric devices in organisational settings their advantages, disadvantages and actual and potential abuses from the point of view of critical theory. From the perspectives of Panoptic surveillance and hegemonic organisational control, the paper examines the issues related to privacy and identification, biometrics and privacy, biometrics and the 'body', and surveillance and modernity. The paper also examines the findings of a survey carried out in Australia, Malaysia and the USA on respondents' opinions on the use of biometric devices in everyday life including at workplaces. The paper concludes that along with their applications in border control and national security, the use of biometric devices should be covered by relevant laws and regulations, guidelines and codes of practice, in order to balance the rights to privacy and civil liberties of workers with employers' need for improved productivity, reduced costs, safeguards related to occupational health and safety, equal opportunity, and workplace harassment of staff and other matters, that employers are legally responsible for.

Keywords: Biometric Devices, Workplace Surveillance, New Technologies and Privacy, Organisational Control, Australia, Malaysia, United States, Public Opinion on Biometric Devices

Introduction

IN SEPTEMBER 2004, a proposal was made to regulate workplace surveillance in the state of Victoria, Australia, suggesting that employers should seek prior approval from a special agency before using technologies to 'spy on their staff'. In another proposal, the Victorian Law Reform Commission wanted to make employers comply with a code of conduct designed to regulate workplace monitoring (Robinson, 2004; 3). These proposals argued that the increasing use of psychological, medical and alcohol testing of employees, the use of tracking devices to locate employees who are mobile workers, finger printing, face recognition technology, camera surveillance, email and Internet monitoring and physical searches within organisational settings, involve privacy concerns. According to the Chairperson of the Commission-Marcia Neave, there were gaps in workers' legal privacy protection, and therefore, providing protection for workers from excessive surveillance needs to be balanced with employers' need to guard against thefts and frauds and maintaining safe work environments (Robinson, 2004).

In recent times, employee surveillance procedures worldwide have been increasingly adopting biometric devices in the name of improving productivity and security. Previously limited to high security facilities due to their high cost and other limiting factors, today, biometric systems have become more compact and less expensive due to their wider diffusion-especially since their adoption in passports and other documentation related to air travel and border control (David, 2004). They are best known as linked to the US government's requirement for biometric passports and visas for travel to the USA, imposed after the September 11, 2001 terrorist attacks on New York City (SBS Online, 2003). This situation has accelerated the diffusion of biometric devices and changed their status from being a niche technology to one that is ubiquitous (Kochan, 2004; Economist, 2000). Just like the governments and law enforcement authorities in countries such as Australia, Malaysia and the USA (Weerakkody 2004 & 2005) which are using biometrics for surveillance purposes of their citizens and others in the name of security and efficiency, employers worldwide too have been able to justify and carry out their implementation, without much discussion, debate,
accompanying regulations or legal and ethical guidelines.

Rationale for the Study

McGinty (2005) reports on a survey of more than 800 people from 21 countries in Europe, Africa and the Middle East, conducted by Hitachi Data Systems which found that Information Technology (IT) professionals expect the adoption of biometric devices in their own workplaces, to be commonplace within two years. More than half of those surveyed had suggested they would resist their implementation while the others saw it as ensuring security. About 25% of the respondents were concerned about the vulnerability of the technology and the potential abuses of the data collected using them, once adopted by employers. Reports from many countries indicate that organisations are increasingly using biometrics to keep track of even their white-collar salaried staff in a bid to reduce staff costs and maintain disciplinary control. This process often leads to violations of employees' privacy or even civil liberties (Maher, 2003; Phillips, 2004; EPIC, 2004; Clarke, 2001). Most often, the justification for their use is organisational efficiency, improving productivity and maintaining staff safety. Therefore, it is important to examine the characteristics of biometric devices, their uses and abuses and what members of the general public—many of whom will be employees themselves, feel about the use of biometrics in their workplaces in everyday situations, that directly affect them. The study involved three countries viz. Australia, Malaysia and the United States in an effort to compare the differences between them in the opinions expressed on the matter due to their cultural differences, as well as their current wide adoption of biometrics (Weerakkody, 2004 & 2005).

Advantages of Using of Biometric Devices in Organisational Settings

Some proponents of biometric devices see them as a 'friend of privacy' (Woodward, 1997) as opposed to the Orwellian 'Big Brother' (Orwell, 1949) or Foucault's Panopticon (Foucault, 1977) of surveillance (Miller, 1971). They claim that biometrics which are unique to an individual, provide 'foolproof' and positive identification that cannot be faked, lost or stolen like passwords, signatures or Personal Identification Numbers or PINs (van der Ploeg, 2003). Using biometrics for tracking employees can reduce overtime abuse, calculate employee hours more accurately, eliminate 'buddy punching' (where others punch cards for those absent) and help calculate staff productivity in manufacturing in terms of the number of units completed within a given time interval (Maher, 2003). These employers believe the technology would help identify the 'good' and 'bad' workers in an organisation more effectively. In short, biometrics are seen as improving efficiency and convenience for both staff and employers, as suggested by the optimistic or utopian view of technology (Hirschhiem, 1985; McLuhan, 1969).

Defining Biometric Devices

Biometric devices or identifiers provide a methodology for (automatically) determining authorised persons' access to facilities and services (instead of via passwords etc.) using their unique individual physiological or behavioural characteristics (Smith, 2003; 34). Biometrics are used for identity verification of an individual as a one-to-one comparison between the person's biometric (measurable biological characteristics of a living person) provided at the time of verification, with the person's own biometric stored in a database or a smart card.

The most commonly used physiological biometrics are facial features, vein patterns in the retina, iris scans, finger prints, palm prints, hand shape etc. Behavioural biometrics include voice analysis for cadences, pitch etc., signature dynamics, and keyboard typing rhythms (Smith, 2003; Lockie, 2002). The less commonly used physiological biometrics are body odour, finger length, knuckle creases, fingertip structure, ear and lip shapes etc. While movement gait can be used as an additional behavioural biometric. These characteristics are considered unique for an individual and some will be different even between identical twins.

Even though unique for each person, DNA is not classified as a biometric identifier as its testing is not yet fully automated (Lockie, 2002).

Applications of Biometric Devices in Organisational Settings

The Economic Advantage Corporation, a mortgage services company in Woodstock, UT and Manhasset, NY, requires its 35 strong staff to use fingerprint recognition for attendance tracking. This has resulted in the company's Client Services Representatives getting paid by the hour even though they are salaried staff, by not paying them unless they worked the full number of hours required (Maher, 2003).

Illiana Financial Credit Union in Calumet City, IL, has used fingerprint scans to track its tellers and loan officers since 2001. The system has allowed the company to save 10-15 minutes a day per staff member in wages as the system records the exact
times worked, rather than approximate durations as when staff fill out their time sheets (Maher, 2003).

In Tâhlequah, OK, the Tri-B Nursery – a plant wholesaler, uses a hand recognition biometric system instead of punch cards to track its 500, mostly immigrant workers across its 300-acre property during busy seasons. This helps them move the workers around the property more efficiently, than when using walkie talkies (Maher, 2003).

However, there is mounting suspicion about these technologies currently being used by employers as tracking and surveillance systems rather than for increasing productivity, safety or efficiency (Glover, 2004).

Abuses of Biometric Devices in Organisational Settings

Clarke (2001) represents the pessimistic view of technology (Herschel, 1985) when discussing the negative implications of biometric devices for human rights and privacy. He argues that biometrics enable powerful organisations to exercise social control over their employees and the systems’ designs have neglected the interests of the individuals upon whom they are imposed. When combined with other surveillance technologies, biometrics can allow organisations and employers to exert enormous power over their employees. Faced with situations where staff may be compelled to use the biometric technologies in order to be employed, employees will be less willing and able to protest against or resist their use in spite of their negative repercussions to themselves. Individuals being forced to submit to ‘technological imperatives’ over those of individual privacy and civil liberties, can lead to an organisation or society that is less open and free (Clarke, 2001).

Supporting this view are Maher’s (2003) examples of paralegals and receptionists at a legal firm in New York who are required to clock themselves in and out of office, using a fingerprint scanner, which allows their managers to know ‘how long’ each employee spent on his or her lunch break. The employer claims that the system has made staff more conscious about getting back to work on time after their breaks and that it has been very successful in boosting productivity.

In South Korea, a biometric using the vein pattern in the wrist has been introduced in government offices, universities and companies at a time when the previously used fingerprint scan was removed due to public criticisms about their use. This new device is intended to ‘maintain organisational discipline’, recording attendance and overtime more effectively, improve efficiency and simplicity, in comparison to the previously used card recognition system (Youhap English News, 2005).

Workplace rights advocates argue that such surveillance and tracking is needlessly invasive unless carried out due to specific reasons that make the tracking and surveillance necessary (Maher, 2003). Others argue that the practice of surveillance and tracking negatively affects staff morale and lowers productivity (Eisenberg & Goodall, 2004).

Time and attendance tracking of employees with biometrics, is seen as a ‘persuasive management tool’ by some employers, because managers can use comparisons of staff hours across time (or various workers) to make an argument about a worker’s productivity and improvement or otherwise. The practice of tracking time is fast being extended to white collar and salaried staff in recent times (Maher, 2003).

In addition to reducing overtime abuse and improving scheduling, managers can also use biometric tracking to catch ‘lazy’ workers—generally non-unionised shift workers who can choose their days worked. In practice, most employers use this tracking to find evidence such as late attendance to build a case against specific staff in a bid to get rid of them, instead of using the data exclusively for payroll functions, as suggested with time tracking and overtime abuse (Maher, 2003).

Theoretical Framework

The main theoretical basis for this paper is critical theory, according to which it is necessary for a researcher to examine the positives and negatives of the adoption of this new communication technology within an organisational setting, in order to highlight whose interests are served in the process and who may be disadvantaged and how, and to provide suggestions as to what should be done to remedy the situation (Eisenberg & Goodall, 2004). Uncovering the hidden power of organisational systems and structures is a central focus of critical theory (Eisenberg & Goodall, 2004). As Habermas (1972) points out, social legitimation (eg. of the use of biometric devices) has a major function in keeping contemporary organisations held together, when they implement a technology that is socially accepted such as within the context of international terrorism worldwide (for security) or global competitiveness (in terms of staff productivity and reduced costs). Accordingly, the ‘manufacture of consent’ (Herman & Chomsky, 1988) of the employees (by the more powerful organisation) makes employees at all levels willingly accept, adopt and enforce the legitimate power of one’s organisation, society and systems of capitalism. This applies to biometrics since their use is often justified and framed as improving productivity and reducing costs, waste, theft and fraud. Such arguments are hard to oppose as they are
presented as directly benefiting the organisation, its employees and other stakeholders, even if the technology can violate the privacy and freedoms of the employees in the process.

According to Dennis Mumbey (1993), the main principle of critical theory is that ‘organisations are not neutral sites of sense-making, and are created within the context of competing interest groups and systems of representation’ (p.21). Antonio Gramsci (1971) uses the term ‘hegemony’ (dominance) to describe the hidden power of society. Society includes or surrounds the power of rules, standard operating procedures and routines (a sequence of unvarying instructions of performing a task) which help maintain discipline within an organisation, which most managers work hard to maintain. This gives rise to the belief among employees that their behaviour is not controlled by other people such as managers, but by the organisation. It may result in staff thinking that ‘this is how management wants things done’, instead of ‘this is how management wants things done’ (Mumbey, 1993).

New communication technologies can also help power holders in society to maintain their hegemonic power or dominance over society (Beniger, 1985). This is achieved by keeping individuals or even groups under surveillance, such as with video cameras, and biometric devices, as argued by the pessimistic view of technology (Hirschheim, 1985) based on the principle of Michel Foucault’s (1977) ‘Panopticon’ with its wheel configuration or George Orwell’s (1949) ‘Big Brother’ with reference to ‘emerging informational practices’ (Phillips, 2004; 695).

Mumbey (1993) further argues that routines are rarely negotiable and most often are not to be questioned or up for redefinition by members, who are expected to follow them as part of their work. For example, when biometric devices are implemented within organisations, employees may not be fully aware why they are necessary or what they are really meant for, but may not be in a position to question or resist them in a meaningful manner.

**Literature Review**

Before the September 11, 2001 events, discussions on biometric devices had been about physical and data security. At the time, biometrics were mostly a feasible and convenient method for accessing PCs, notebooks, networks and data. But since September 11, their use has been radically transformed and used with physical access and surveillance as the main goals of implementation, due to issues related to homeland security and border control to protect against international terrorism (Essex, 2003). However, civil liberties advocates fear these data will be used by law enforcement authorities to spy on innocent citizens, due to the lack of adequate legal guidelines and legislation to keep them under check (O’Harrow, 2005). The increasing and regular use of biometrics in workplaces adds to this fear of misuse.

Biometric access devices have four common applications (Essex, 2003). They are i) Control of access (to IT resources and buildings), ii) Screen (to validate people at social service organisations, airports, border control etc.), iii) Surveillance and iv) Law Enforcement (identifying crime suspects via databases of fingerprints etc).

In the past, fingerprints were used for those suspected of crimes and carried out by law enforcement authorities, under strict rules and guidelines. But today, many organisations and employers routinely use them for staff identification and tracking. Some may see this as overuse of the technology, which may be utilised by employers more for control than security and efficiency.

**Privacy and Identification**

Alan Westin (1967) defines privacy as the right of individuals, groups and institutions to determine for themselves, when and how and to what extent information about them is communicated to others. Privacy is not about hiding from others, but about controlling the flow of information of one’s personal data (Lumeria, nd. cited in Phillips, 2004)

Phillips (2004) argues that the term ‘identification’ is an overloaded word just like the term ‘privacy’. According to him, identification can be of three types viz i) *Lexical* (where a name is linked to an entity), ii) *Indexical* (points to where a particular entity is linked to a particular time and place helping to track and find the person) and iii) *Descriptive* identity (assigning attributes to an entity in a particular time and place in relation to other entities, such as according to a profile). Descriptive and lexical identifications are linked to surveillance and create social norms (eg. defining who is a ‘slacker’ in a given organisation) and fields of knowledge (eg. What do we know about his ‘slacking habits’ in comparison to those of ‘diligent’ ones?). Indexical identification is linked to panoramic normalisation and surveillant social coordination, and therefore linked to ‘intrusion’ (Phillips, 2004).

Economist (2003) argues that contrary to popular belief, and given the limitations of biometrics due to their fallibility, unreliability and susceptibility for forgery (Economist, 2000), the ‘Big Brother’ concerns of privacy advocates is currently somewhat misplaced, because other surveillance technologies such as Internet wire tapping, tracking of mobile phones and Global Positioning Systems (GPS) to
locate vehicles, pose a larger threat to privacy in the foreseeable future. But in the long run, biometrics can compromise privacy in a deep and thorough fashion (Economist, 2003).

However, privacy advocates argue that benefits of biometrics related to productivity, fraud and identity theft reduction are not worth the risk of ‘function creep’ (Economist, 2003; Weerakkody, 2005), where once biometrics are used for one purpose, they can be used for all others such as routine access to work computers in ordinary day to day businesses etc.

Eisenberg & Goodall (2004) found employee responses to electronic monitoring of productivity where frequency and speed of work is measured, stored and reviewed by management, as mixed. Some see it as an invasion of privacy while others see it as giving performing greater recognition for their work.

**Biometrics and Privacy**

Biometrics give rise to issues of privacy and civil liberties due to aspects related to Storage (How the data are stored – are they stored centrally or dispersed?; How can the data be retrieved?); Vulnerability (Can they be stolen or abused?); Authenticity (Can the information be tampered with?); Linking (Will data gained in one area be linked to other information about someone? What are the limits to others’ use of this information?); and Ubiquity (the implications of having an electronic trail on someone, when multiple surveillance technologies are used to gather information on that person and such technologies are commonplace) EPIC (2004). These concerns can be applied to biometric data collected by organisations on their employees where privacy and even civil liberties violations can occur due to abuse and misuse of the data collected on staff.

The argument that biometrics can actually protect privacy instead of violate it, is based on their potential to allow verification of identity in transactions and delivery of services without disclosing the person’s name, address and other personal data and because encryption can secure and protect identities (van der Ploeg, 2003). However, one could also argue that using passwords and PINs carry out the same function.

In opposing the implementation of biometrics in Korean organisations, an editorial in the Youhap English News (2005) argued that as biometrics provide unique and sensitive data that identify a person’s personal characteristics, their abuse can lead to serious privacy violations and social discrimination. Therefore, biometric devices should be implemented very carefully and with much preparation to avoid civil rights abuses and surveillance of labour.

**Biometrics and the ‘Body’**

Most debates about biometrics relate to privacy issues from the perspectives of policy and law rather than from the perspectives of philosophy or ethics. When biometrics are framed as ‘invasive’, it uses the metaphors and analogies of medicine and interventions into the ‘body’. However, biometrics only use the human body’s surface, such as taking photographs, scans and fingerprints, which are non-intrusive in reality (van der Ploeg, 2003).

Those who are subject to biometric identification, also refer to the devices as ‘unhygienic’ (Piazza, 2005) and harmful (to the eye during iris scans), using the same metaphor and analogies mentioned above. In reality, the invasion is related to personal privacy or the ‘life-sphere’ or ‘unreasonable search’, which does not fit the medical metaphor or the concept of the ‘body’ in the same way, since their ‘invasion’ relates to ‘ informational privacy’.

In a survey of 300 respondents carried out in the USA, Moody (2004) found public perceptions of biometrics to be diverse. Many saw them as having the potential to invade personal privacy and no more efficient than passwords or PINs. In general, respondents were not ready to use biometrics. She suggests consulting with staff about their fears and misconceptions and to make sure the devices are feasible and suitable for use by the organisation, before biometrics systems are implemented. Requiring managerial staff also to use the devices, can help minimise the stigma and suspicions attached to them.

**Surveillance and Modernity**

George Simmel- the German sociologist and author of ‘The Metropolis and Mental Life’ stated that ‘the hallmark of modernity (of the early 20th century) was the anonymity of urban life, which made the great cities the locale of freedom. But by the beginning of the 21st century, the hallmark or postmodern society has become the ‘cybernetic cage’ of surveillance. It takes less and less effort each year to know what we are about’ and the details of our own lives are no longer our own. They belong to companies that collect them and the government agencies that buy or demand them in the name of keeping us safe. Therefore, it is up to us to decide on the price we are willing to pay for that promise of safety (O’Harrow, 2005, cited in Stern, 2005 page number n.a.).

O’Harrow (2005) in ‘No place to hide’, points out that the new security systems implemented as a reaction to September 11, 2001 events (that includes
the widespread use of biometrics) will impact on our
traditional notions of civil liberties, autonomy and
privacy and examines how they threaten to
undermine some of our society's most cherished
values, even while offering us a sense of security.

Methodology

This study used surveys returned by 230 individuals
in Australia, 408 in Malaysia, and 300 in the USA
who were a part of a convenience sample selected
via the researchers' personal contacts and their
acquaintances, during 2003 and 2004. 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 fingerprint as unsanitary)
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
above-mentioned five preferences, would make them
feel uncomfortable or reluctant to use. In addition,
there were three open ended questions posed to the
respondents viz. 'I currently use the biometric
devices in the following ways', 'My concerns about
using biometric devices are' and 'I think we should
use biometric devices to'.

However, this paper reports only on a comparison
of responses for the items that asked the respondents
if they thought 'Biometric devices are an invasion
of privacy', 'Biometric devices are a good way to
keep track of employee work hours' and 'which
biometric devices such as fingerprint scans, iris
scans, retina scans, voice recognition and
handwriting recognition, they preferred to gain access
to their offices'. The respondents could choose any
number of devices from the list provided, with the
last item.

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. However, the US surveys did not
include the item on the level of education of
respondents.

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 the four age groups listed in the
survey etc.) (Baxter & Babbie, 2004). Based on this
breakdown, the researchers used convenience
samples of suitable individuals within these groups
drawing on respondents from those among and with
the help of their acquaintances in Australia and the
USA. The Malaysian data was collected by a
Malaysian-based associate of one of the researchers,
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. An analysis of the US data, examined
from the point of view of public acceptance of
biometrics, was reported in Moody (2004).

Weerakkody (2004) reported a preliminary analysis
of the Australian data examining responses to the
survey's open ended questions while Weerakkody
(2005) compared Australians' and Malaysians' view
on the use of biometric devices in everyday
dimensions, also using their responses to the open
ended questions.

Demographic Distribution of
Respondents

Even though efforts were made to obtain the
responses from equal numbers of people from the
two sexes and 25% each from the four age groups,
the number of returned surveys for Australia included
38.7% from males and 58.6% from females. The
sample for Malaysia consisted of 38.5% males and
60.8% females while the figures were 61.7% males
and 36.3% females for the US sample.

In terms of age groups, Australian surveys were
distributed as 37.8% coming from respondents in the
10-20 age group, 25.65% between 21-30 years of
age, 25.21% as between 31 and 50 years old, while
8.7% were over 51 years of age. The Malaysian
respondents were distributed as 11.2% from the 10-20
year old group, 66.7% between 21-30 years of
age, 21.3% from the 31-50 year group and 0.7% from
those over the age of 51. The American respondents
were distributed as 3% between 10 and 20 years of
age, 43.3% between 21-30 years of age, 41.3% from
those 31-50 years of age and 11.7% of those over 51 years.

In terms of education level, data are only available for Australia and Malaysia. The respondents were distributed in Australia as 15.7% with some high school education, 12.2% with high school diplomas, 23.9% with some university education or trade certificate, 27.8% with university degrees and 16.5% with postgraduate qualifications. For Malaysia, the breakdown was 4.9% of respondents with some high school education, 9.5% with high school diplomas, 12.3% with some university education or trade certificate, 60.5% with university degrees and 8.8% with postgraduate qualifications.

A few survey respondents had not provided all their demographic details, which explains why the percentages given above for some categories and countries do not always add up to a 100%.

'Biometric Devices are an Invasion of Privacy'

When analysing the responses given by the respondents to the question, 'biometric devices are an invasion of privacy', of those responded, 33.0% in Australia, 19.1% in Malaysia and 52.7% in the USA either strongly disagreed or disagreed with the statement. Those neutral on the issue were 38.3% in Australia, 18.7% in Malaysia and 25.7% in the USA. However, 27.8% in Australia, 60.1% in Malaysia and 21.4% in the USA either agreed or strongly agreed with the statement.

Given that the Malaysian sample consisted of a much higher percentage of those with university degrees or higher, their response to the threat to privacy from biometric devices is understandable, in comparison to those in Australia and even the USA. Malaysia is the first country in the world to introduce biometric passports and is trialling the MyKad as a multipurpose biometric identity card (Weerakkody, 2005). Even though a democracy, Malaysia also had an authoritarian government under its former and long time Prime Minister Dr. Mahathir Mohammad. At the same time, one must take into account the characteristics of respondents who volunteer to take part in any survey as being different to those who do not (Baxter & Babbie, 2004). Many respondents who do not like the use of biometrics in everyday life, may have been more interested in returning the surveys to have their voices and concerns heard, than others.

'The Preferred Biometrics to Access Offices'

In response to the survey item that asked respondents which biometrics they would 'prefer to use to access their offices', the choices offered were finger print scans, iris scans, retina scans, voice recognition and handwriting recognition. Respondents were free to choose as many as they liked, from the five listed.

A cross tabulations obtained indicated that the five biometric devices were preferred by the respondents in the three countries, as follows.

Fingerprint scans:
The yes vote from Australia was recorded by 54.3% of respondents. For Malaysia, 57.1% said yes, while in the USA, the preference was 57.3%.

Iris scans:
For Australia, the preference for iris scans was 17.4%, while it was 12.3% for Malaysia and 12.3% for the USA.

Retina scans:
The preference among Australian respondents for this biometric was 14.8%, while it was 14.2% for Malaysia and 20.3% for the USA.

Voice Recognition:
From the 230 respondents in Australia, 25.7% preferred voice recognition, while 13.0% in Malaysia and 29.5% in the USA did so.

Handwriting recognition:
This biometric recorded the lowest preference from respondents in all three nations. The figure was 4.3% for Australia, 5.1% for Malaysia and 4.0% for the USA.

Overall, this study indicates that Malaysians were the group which saw biometrics as violating privacy the most, while fingerprinting was the preferred biometric for all three countries when accessing their offices. Voice recognition was second most preferred for both Australia and the USA, while retina scans were second most preferred by Malaysians.

Future Directions
This study is a preliminary cross-cultural examination of how citizens of three multicultural nations perceived the use of biometric devices in their everyday lives. Therefore, the dependence on a convenience sample was suitable for the purpose. However, such a sample limits the generalisability of the findings and the scope of the study. To be able to make more in depth analyses and interpretations of the data gathered via such a survey used in this study, one can use random samples to examine the perceptions of biometrics in these countries. To
examine how the variances in responses may be explained as due to their cultural, political and social differences and realities, further research may be necessary.

Just as seen in Weerakody (2005) that examined the responses of Malaysian and Australian respondents to the three open ended questions, this study indicates some differences between the perceptions of biometrics as invading privacy in the three countries, which need further study. Such further research could include interviews with members of the public who do as well as those who do not have experience with using biometric devices; those who support as well as oppose the use of biometrics in everyday life; vendors of the technology; policy makers and government officials in charge of implementing the technology and related policies; privacy advocates; trade union officials; 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, employers, policy makers, government officials, workplace and privacy advocates and trade union officials- with respect to the use of biometric devices at workplaces to track employee work hours and for other purposes of surveillance.

Discussion

Stern (2005) points out that the founding principle of the American Republic (as well as in Australia, Malaysia and other democracies) is ‘inefficiency’ due to the existence of bicameral legislatures, an independent judiciary, an independent executive and the separation of their powers to keep each arm of government in a position to check each other. This can be seen as ‘inefficiency’ and slow, as processes need to go through various stages and scrutiny by the various arms. On the opposite side lies the founding principle of the industrial revolution, which is based on ‘efficiency’. These two principles had been ‘at war’ since the creation of the American republic.

The ever lowering cost of energy (water power, steam and then electricity) moved the agrarian society of the 18th century into an urban, factory-based world in the mid 20th century. The situation today is somewhat similar, due to the increasingly lowered cost of information in a globalised, network-based, post-industrial economy in the information age. In this ‘efficient’ set up, all that was ‘inefficient’ or the checks and balances deliberately included in a democracy, are eliminated by technology, which moves at a much faster rate than laws and regulations related to them, making it difficult for laws and regulations to keep up with technologies and their advances. As a result, new information technologies have been able to eliminate or circumvent the very liberties these ‘inefficiencies’ were designed to protect. This interplay between privacy and information technology within the context of the ‘efficiency’ of the information age, has created many discontents (O’Harrow, 2005, cited in Stern, 2005).

David Gregory, Director of the Victorian Chamber of Commerce and Industry Workplaces in Australia, points out that one should not consider privacy issues related to employee surveillance in isolation, as surveillance may be necessary to deal with matters related to Occupational Health and Safety (OHS), sex discrimination, and equal opportunity. Monitoring workplaces and testing workers can help organisations guard themselves against possible future legal claims (cited in Robinson, 2004).

However, it is necessary to win the support of the users to ensure a biometric system is used properly and not sabotaged (Kochan, 2004) and to impose guidelines and codes of practice for their implementation and use. In addition, laws and regulations must be in place to guarantee that the technologies and the data they collect are not abused by managers or employers, to discriminate or oppress workers.

Conclusions

In order to dispel fears of privacy abuses, the International Biometric Industry Association (IBIA) code calls for legislation to control the use of biometrics. However, it would leave private industries to self regulate voluntarily (Wadman, 1999). This self regulation cannot be guaranteed of all private industries, especially since the technology is becoming more affordable. In an environment of cost cutting, improving productivity, and ‘discipline’ of workers, employee surveillance and efficiency can take precedence over all other considerations, including individual privacy and civil liberties.

Biometrics and other surveillance technologies may be able to measure the time an employee spends at their desk or post. But being at one’s desk or post only allows certain levels of productivity and tracking hours worked is only an incomplete measure of it (Maher, 2003). Such surveillance can give rise to a work environment that lacks flexibility and creativity, as well as one that allows little room for individual and personality variances (Maher, 2003).

Privacy advocates worry that digitised identification systems can be easily abused by governments and industry. As seen since September 11, 2001 in the USA, governments can also seek to access databases of information on private individuals from private industries and organisations for intelligence, law enforcement and other purposes.
(Stern, 2005), giving rise to ‘function creep’ (Economist, 2000; Weerakkody, 2005). The US Government had found this situation to be convenient, efficient and a way to circumvent legal restrictions imposed on it in collecting and maintaining such databases, which do not apply to industry (O’Harrow, 2005). One could fear that biometric data collected by employers, especially large organisations, could one day be obtained by governments and used in a way to disadvantage the individuals concerned. Such surveillance ‘dulls the edge of public debate, imposes a sense of conformity, and introduces an uneasy feeling of being watched. It dulls the culture and stifles dissent. Such surveillance by definition is often secret and hard to hold to account’ (O’Harrow, 2005 cited in Stern, 2005, page number n.a.).

Jim Dempsey – the Director for the Center for Democracy and Technology sees the ‘unprecedented intrusion’ into American life that resulted after the passing of the US Patriot Act in 2001 (cited O’Harrow, 2005). Applying O’Harrow’s views on the effects of electronic surveillance on ordinary citizens and to the implementation of biometric surveillance in workplaces to observe and measure staff productivity, work hours and ‘misbehaviours’, one can argue that biometrics can support ‘electronic searchers’ without the knowledge of the individuals being monitored. In an organisational setting, they could set social norms as to ‘who is a good worker and who is not’, not determined by formal performance evaluations but based on what comes up on the managers’ computer screens (O’Halloran, 2005).

In conclusion, I would argue that instead of increasing productivity, biometric surveillance can lead to the opposite effect due to low staff morale and loss of motivation, leading to fears of taking initiative or responsibility. They can lead to feelings of powerlessness, being under excessive control, and not being trusted by their employers and managers.

As Steve Bracks – the Premier of the state of Victoria in Australia has pointed out, ‘A ‘human capital’ agenda (followed by employers in valuing and trusting their employees) will ensure a healthy, skilled and motivated (workforce and) community, delivering greater productivity and higher labour force participation’ (Bracks, 2005; 16).

Acknowledgements

This paper is based on a study that examined public opinion on the use of biometric devices in everyday situations in Australia, Malaysia and the USA. The study and its survey instrument were designed by Associate Professor Janette Moody of the Citadel, Charleston SC, USA, while the author served as co-investigator. The author wishes to thank Dr. Jamilah Ahmad of the 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.

References


About the Author

Dr Niranjala Weerakkody
Niranjala Weerakkody, Ph D, Rutgers U, NJ, USA is a Senior Lecturer and Associate Head at the School of Communication and Creative Arts at Deakin University.