NO AGE DISCRIMINATION FOR BIOMETRICS

[1]M.M. Lessing and L. Weissenberger

[1]Council for Scientific and Industrial Research (CSIR)
[1]marthie.lessing@gmail.com
PO Box 923, Ferndale, 2160, South Africa

ABSTRACT

Biometric advances apply to a range of disciplines to ensure the safety and security of individuals and groups. To stress the value of biometrics, this study focuses on the application of biometric techniques to a vast range of individuals and groups, irrespective of their age. This report covers biometric development within three generations.

For the younger age group, biometrics can play a significant role in ensuring physical safety within the learning and dormitory environment. Additionally, biometrics can assist teachers within this environment to enhance the administration features. This allows more hands-on time for the education of children.

The application of biometrics for adults has made great progression in the last couple of years. The research considers biometric advancements in the areas of travel and immigration, healthcare, law enforcement and banking. For the purpose of this study, adults are considered the individuals and groups in a working environment. Many of these applications are relevant to the younger and more senior generations as well.

Senior citizens can also benefit from biometric applications. In many countries, biometric techniques control the administration of pension funds and general welfare administration.

For each of the biometric applications, this research reviews the application of biometrics, associated advantages and disadvantages, as well as specific implementations. A number of sample applications from all over

the world, illustrates the usability of biometrics for a variety of groups, individuals and disciplines. From this report, it is clear that biometrics is a universal application, used by anyone, anywhere.

KEY WORDS

Biometrics, safety and security, school environment, travel, immigration, healthcare, law enforcement, banking, pension funds.

NO AGE DISCRIMINATION FOR BIOMETRICS

1 BACKGROUND

Biometrics is not a passing fad, and definitely not a new development. The earliest recorded use of biometrics for identification purposes occurred during the 14th century. This is when Chinese merchants stamped children's palm and footprints with ink on paper. The year 1881 was a noteworthy milestone in the advance of biometrics: Alphonse Bertillon developed an anthropometric system that measures and distinguishes between human traits (AB 2006). It is, however, only in the last 120 years that the biometric discipline introduced drastic changes (Arnold 2006).

The application of biometric techniques has slowly infiltrated our daily lives and has established an intimate interdependence between humans and technology. In computer security, biometrics refers specifically to automatic authentication techniques relying on physical measurable features. Biometrics refers to: "… technologies that measure and analyse human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes" (SearchSecurity.com 2006). The use of biometric applications has become so prevalent that AuthenTec, the world's leading provider of fingerprint sensors and solutions, reported a 67 percent increase of biometric related sales in 2007 (FindBiometrics 2008a).

In No age discrimination for biometrics we attempt to show that biometrics has infiltrated all facets of human life, with specific attention to the security aspects. We discuss biometrics for the young, for adults and for senior citizens and prove that no matter what your age, there is a biometric application that applies to your needs and circumstances.

2 BIOMETRICS FOR THE YOUNG

Children are the world's future, and it is very important to keep them safe. Since majority of children attend schools and many youths colleges and universities, this section addresses the application of biometric techniques in the learning environment.

2.1 Educational institutions

Schools are supposed to be a secure haven where children can achieve their full potential, but are schools as safe as we want to believe? In order to learn and excel, scholars need to feel safe in an environment where they can focus on their studies. Not only the learners' and students' safety is important, but teachers and lecturers also need to know that they are in a protected environment where they can focus on the curriculum.

Existing security solutions are far from perfect. Children have the knack to lose physical keys and magnetic swipe cards, forget passwords or fall victim to the social engineering skills of school bullies to obtain lock numbers. In addition, the current process to gain secure access to school grounds is both time consuming and ineffective. The most probable solution is a reliable access control and identification system, combined with effective entry policies.

2.1.1 Application areas

It is seldom that all the relevant parties immediately accept the introduction of a new technology. Especially in the teaching and learning environment where minors are involved, people become natural sceptics. Yet, with the young generation's outlook on technology and inventions, it is not surprising to find a great variety of biometric applications in school environments.

The best way to introduce biometrics in educational institutions is to prepare an alternative system for individuals uncomfortable with the new system. This will get the approval of the students, their parents and the educators (Goldberg 2003).

The most common application is campus access. Access is limited to preferably one entrance equipped with a biometric scanner to verify the identity of all students, staff and authorised visitors upon entry (Goldberg 2003). The execution of biometric systems in schools should be relatively easy, since children seem to hold no fear of new technology. More than 1,300 UK primary schools' libraries are using fingerprint technology to replace the old-fashioned password systems. More children now borrow books because they want to use the new technology (Out-Law News 2004).

Another application that can speed up scholar attendance registry is placing cameras throughout the school, authenticating students looking into the camera. Roll call information is available immediately, and not only after first break as is presently the norm with class attendance lists (Nixon 2003). Students can also use their biometric features to authenticate themselves on the school network by logging on to a wireless network. The application of biometrics leads to tremendous time saving (Goldberg 2003). For students with medical allergies, biometric devices have proved to be lifesavers. School nurses use fingerprint scanners to identify sick students and their allergies before they administer medication (FindBiometrics 2003).

For schools with a vision to send pupils into the business world equipped with all the necessary skills, biometric school environments are ideal. The school environment introduces the technology to students in an informal environment, and prepares them adequately for biometrics in a more formal corporate world. In addition, the use of biometric technology in the classroom will leave both the scholar and the teacher feeling more secure in the school environment and will enhance the learning experience (BIOMETRICS in Education 2004).

2.1.2 User resistance

The main problem with using biometrics in educational institutions is people's resistance to change (in this instance the school/university staff and parents), their resistance specifically to biometric technologies and the cost implications of such technologies. Though expensive, the arguments in support of biometrics weigh much heavier. Privacy concerns may put a dampener on acceptance rates, but should not prevent biometric technology from reaching its full potential in security enhancements (Goldberg 2003). Educational institutions already hold the responsibility for sensitive data such as identification numbers and special needs information. Biometric systems simply add additional information to these personal data files.

Additionally, there is a worldwide fear by school employees of contracting diseases from using the same scanners as the scholars. Children can pass on childhood diseases that could hold immense danger for adults and their families. The likelihood of open cuts and the transfer of germs is

another concern, but according to Borja (2002) the risk of contamination is minimal to nonexistent.

Advocates in support of biometrics in schools say that the resistance endures because the technology is misunderstood. Finger scanners do not record actual fingerprints and is of no use to law enforcement (Graziano 2003). Once the resistance has subsided, biometrics can enhance the school environment with access control, positive identification and a record of those entering and leaving school buildings. Hopefully the fears of identifying information misuse will soon be forgotten to embrace the benefit of enhanced accountability (Goldberg 2003).

2.1.3 Advantages and disadvantages Application areas

The advantages of a successfully implemented system include saving on administration costs, increased accountability, improved building and data security and improved effectiveness in administrative tasks. With minimal biometric training required, this technology relieves teachers of their administrative tasks, leaving more time spent teaching (BIOMETRICS in Education 2004).

The greatest benefit of biometric authentication is that students can display their fingertips publicly without any threat of compromising their accounts' privacy or the network's security. It is also highly impossible for a student to authenticate using someone else's fingertip, or forgetting their fingertips (Kennard 2002). The most disabling disadvantage of biometric systems in the educational environment, however, remains user resistance by educational administrators.

2.1.4 Biometric implementations in schools worldwide

Biometric implementation on school grounds have been surfacing slowly since late 1997. The following are a few examples of educational institutions that implemented biometric systems successfully:

- At the Kvarnby School, Stockholm it generally takes half a period before teachers could help all children sort out their passwords problems. Some students forget the passwords, while others borrow user names and passwords from other students. Often the default password is never changed and written on the blackboard, completely negating the use of passwords. A fingerprint-based

solution eliminated these identification problems, making the login routines easier and saving valuable classroom time (Security International 2002). At Johnson and Wales University, Denver, students no longer need to worry about lost access cards or residence room keys locked in, nor the fines associated with such occurrences. Students entering the Pulliam residence need only to slide their hand into the biometric hand reader for the door to open. The room doors work on the same system (Johnson & Wales University 2002).

- Since 1993, the scholars at the Penn Cambria schools have registered by means of their fingerprints. Only students who have recently transferred to the district and returning students in the fifth and ninth grades need to reregister due to a growth spurt. At these ages, children's fingers have matured to the point where the scanners can no longer quickly identify them. Of around 3000 students, only about 1% opts out of the scanning system due to religious preferences (Graziano 2003).
- US Biometric Corporation, in conjunction with law enforcement experts, are introducing educational seminars to help tertiary institutions understand biometrics. The idea is to assist campuses to increase security proactively for both students and employees (Business Wire 2008).

2.1.5 Summary

Educational institutions need enhanced security features to safeguard learners/students and staff members. By implementing biometric systems, it is possible to improve the current security systems and to boost supporting actions in and around the study environment. Currently many biometric applications serve the global educational environment, varying from simple identification procedures to intense authentication and verification procedures. The advantages of biometric systems far outweigh the disadvantages thereof, and may even lead to a more technology proficient youth.

3 BIOMETRICS FOR ADULTS

The application of biometrics in adult life is a vast field. This section deals with travel and immigration, healthcare, law enforcement and banking.

3.1 Travel and immigration

In the light of terrorist attacks occurring around the world, governments are looking to intensify security controls, especially in the field of immigration. Biometrics is likely to increase security at immigration control points like border posts and airports.

3.1.1 Application areas

Biometrics can assist the travel and immigration industry in two distinct ways: verifying the identity of visitors and including biometric identification within passports. When validating a visitor's identity, the immigration official takes a digital photo of the person to match against the database. The system performs a matching against wanted or missing persons in an attempt to uncover fraudulent applications (US Department of State 2004:1,12).

Most immigration departments also take fingerprints of the visitor to compare these to fingerprints in the database. If the system does not recognise the person's fingerprint, it sends the prints electronically to an off-site facility for further analysis by an experienced latent fingerprint examiner (Biometric Technology Today 2004:5).

3.1.2 Advantages and disadvantages

Biometric technology strengthened confidence in passports and visas, reduced fraudulent activity and continually assists in fighting terrorism. The inclusion of biometric data within passports will have three security benefits:

- immigration officers can verify whether the passport identifies the bearer sufficiently;
- the movements of travellers can be more easily tracked, enabling officers to identify those who breach the conditions of their visas; and

- passports will be harder to forge (Biometric Technology Today 2004:12).

Proponents of human and civil rights have expressed apprehension that the increased security measures are part of an international attempt to keep track of people's movements. In particular, they have concerns about facial recognition since it discloses a person's ethnic and racial background. They also have reservations about the accuracy and reliability of the technology.

Regarding passports containing biometric data, vendors have had a great deal of difficulty in incorporating the microchip into the pages of the passport. The main concerns are the possibility of illicit people attempting to read the information off the chip from a distance, and the compatibility of readers manufactured by different suppliers (Biometric Technology Today 2005:2).

3.1.3 Biometric implementations in travel and immigration worldwide

The application of biometrics in the travel and immigration industry has vast ranges. The following countries employ biometric applications successfully:

- Russia recently issued the first biometric passports for Russians travelling abroad. This passport includes a special photograph and a microchip for digital finger or retina prints (FindBiometrics 2008d). More than 50 other countries have migrated to the use of biometric passports in the past three years (Wikipedia 2008d).
- Singapore employed the LG IrisAccess technology to definitively authenticate visa holders and allow them to enter the country, introducing timesaving of over 2400 percent (FindBiometrics 2008b).
- In South Africa¸ IDTek was awarded a R250 000 contract by Airports Company SA (ACSA) to install Sagem's fingerprint biometric technology in the restricted personnel areas of OR Tambo International Airport. This application will enforce security and increase physical access control reliability (ITWeb 2006).

3.1.4 Summary

Biometrics is an important step for governments to take to stay ahead of terrorists and other lawbreakers. In this industry, it is still in its infancy with many obstacles to overcome, but the results look promising so far, which bodes well for biometrics within the immigration environment.

3.2 Healthcare Industry

Errors in the medical profession could mean the difference between life and death. In the United States, approximately 115 000 deaths occur each year from misidentifying a patient (Schneider 2005:24). By implementing biometric technology, nurses can reduce this number significantly by checking a patient's fingerprint before performing a surgical procedure.

Another major issue within healthcare is fraud. It is common for multiple individuals to use the same medical aid card to receive health benefits, especially when the cards do not contain a photographic image of the insured person (Messmer 2004:17). With the implementation of biometrics, this kind of fraud would be greatly minimised.

3.2.1 Application areas

abroad often employ iris recognition scanning for system access control, ensuring that only authorised doctors and nurses can view confidential patient records. Additionally, these workstations can be fitted with proximity sensors so that if a user moves away from the terminal, the system will log the person out (Dalton 2004:12). Fingerprints are the most commonly used biometric identifier used within the healthcare industry, since most readers are able to read prints through grime (Schneider 2005:24).

Many hospitals traditionally had multiple systems, each requiring different logon credentials. Medical professionals needed to remember as many as six different passwords. In some cases, systems implemented single sign-on to solve this problem. The drawback of such a system would be that compromise of a single logon password compromises the entire system. Hence, using biometrics for authentication instead of a token or password is becoming very popular in the healthcare environment. Biometric technology is much more secure than tokens or passwords (Mansfield 2003:40).

3.2.2 Advantages and disadvantages

Biometrics within the healthcare industry can improve the quality of healthcare, reduce medical errors and decrease healthcare costs (Schneider 2005:22). It can also assist in providing an audit trail, by identifying which staff member supplied care as well as what type of care was provided to a patient (Beyond doors: Securing records with finger flick 2002). The main advantages of biometrics include the combating of fraud and abuse in health care entitlements programmes, the protection and proper management of confidential medical records, positive identification of patients, and securing medical facilities and equipment (Marohn 2006).

Although fingerprint scanners are the most widely used biometric device used within the healthcare industry, this can be problematic in areas where staff are routinely required to wear gloves (Dalton 2004). These areas employs alternative, often more intrusive biometric technologies.

3.2.3 Biometric Implementations in Healthcare Worldwide

Biometrical implementations in health care have been successful in the following:

- A hospital in New York and an ambulance service in Chicago have both implemented an ultrasound fingerprint scanner used during patient registration. This fingerprint is stored as part of the patient's permanent record to ensure that only that person uses the medical aid card. The system has successfully expanded to control access to cabinets containing narcotics (Messmer 2004).
- A common phenomenon is phantom billing, where health care providers bill for services never rendered. Texas addressed this problem by incorporating a biometric smart card-based program that requires both the medical providers and the recipients to authenticate themselves when checking in for service. This system greatly reduced hospital expenditures and improved program integrity (Marohn 2006).
- In the aftermath of the Florida hurricanes in 2002, the USA initiated the e-Life-Card program. Individuals seeking medical care during the hurricanes experienced significant delays and lack of access to their medical information. The program allows first

responders to access critical information by using patients' fingerprints as authenticator (Marohn 2006).

- Poudre Valley Health System, Colorado, previously used PINs to control access to their newborn nurseries. However, many incidents of unauthorised persons gaining access to this highly restricted area occurred. The facility now uses hand geometry readers instead of PINs (Reynolds 2004:16).
- Australia introduced the MethaDose program, employing iris recognition technology to support the treatment of heroin addicts. The program registers patients to detect duplicate enrolees, and to enable authentication for patients that are unable to claim their identity coherently. Registration includes personal information such as name, biometric data, permitted dosage, last and next scheduled dosage, all stored on a central database. The Netherlands launched a similar program to automate and control distribution of vaccines during epidemics (Marohn 2006).

3.2.4 Summary

It is clear that biometrics can be very beneficial to the medical industry by creating a more convenient working environment for staff, and reducing fraud and medical errors.

3.3 Law Enforcement

The legal implications and red tape of police departments accessing inter-jurisdictional systems creates an ongoing problem in identifying and apprehending criminals. Additionally, perpetrators using multiple identities can fool traditional identification systems. If biometric features are used, law enforcement may have more success in this regard, linking multiple identities to a single person. In many regards, it may be beneficial for law enforcement agencies to share biometric data.

3.3.1 Application areas

The first recorded use of latent fingerprints as a means of identification is in 14th century Persia (Wikipedia 2008a). Since then, police departments relied heavily on latent fingerprints and witness reports to identify people that were present at crime scenes. The Integrated Automatic Fingerprint

Identification Systems (IAFIS) is a database system maintained by die Federal Bureau of Investigation, using a one-to-many matching technology to match fingerprints to individuals. IAFIS contains fingerprint and criminal history information for over 47 million people (Patrick 2007).

Since the 9/11 terrorist attacks, there has been major interest in the use of facial recognition software to identify terrorists and other wanted criminals in public areas such as airports, sports stadiums and correctional facilities. Some patrol cars in the United States were fitted with mobile facial recognition units, giving police officers the ability to verify a person's identity within minutes. This is particularly useful when individuals claim they do not have any form of identification on their person. Law enforcement also uses iris recognition to improve efficiency and safety within correctional facilities (Zalud 2003:30).

3.3.2 Advantages and disadvantages

Biometrics has been invaluable as a unique identifying characteristic in determining when a suspect is using multiple identities or aliases (Biometric Technology Today 2005:12). Facial recognition has increased the speed and efficiency of the booking process at police stations, and aided in distributing images and information to other police departments, correctional facilities and sheriffs' offices (Zalud 2003:31).

A major disadvantage of biometrics is that civil liberties groups believe the use of cameras in public streets to constitute an infringement of privacy. They believe that law enforcement should not violate citizens' rights unless they have legitimate cause to do so (Beckley 2004:16). They also question the reliability, effectiveness and correctness of results (Hudson 2003:1) and that these systems could promote racial profiling. Additionally, the use of cameras in city streets has not been as valuable as anticipated since the technology is most effective when the subject is stationary, at close range and when the light is good (Winton 2004). This limits use of the technology, but future improvements should minimise these restrictions.

3.3.3 Biometric Implementations in Law Enforcement Worldwide

Following are examples of biometric implementations in law enforcement:

- The American serial killer Ted Bundy bit Lisa Levy in her left buttock cheek during one of his attacks, leaving prominent bite

marks. A forensic expert positively matched plaster casts of Bundy's teeth to photographs of Levy's wound, leading in part to his conviction (Wikipedia 2008b). The accuracy of this method is highly criticised, since a study done by the American Board of Forensic Odontology revealed a 63% rate of false identifications (Wikipedia 2008c).

- In Florida, police has deployed mobile facial recognition systems in patrol cars. In six months, police made 37 arrests that would not have been possible previously due to the perpetrator providing false or no identification (Biometric Technology Today 2005:12).
- In the United Kingdom, police convicted Mark Gallagher in 1998 of murdering a 94-year¬old woman. The main incriminating evidence was an ear print found on a window at the murdered woman's home. The judicial system overturned this conviction in 2004 when scientists pronounced the ear print evidence flawed, and DNA evidence incriminated another man for committing the crime (Graham-Rowe 2005).

3.3.4 Summary

Biometrics has assisted police departments and law enforcement agencies to capture criminals that they would not have been able to before implementing the technology. It appears that as biometrics becomes more affordable and flexible, biometrics within law enforcement will play a vital role.

3.4 Banking

Despite years of marketing and hype surrounding biometrics as the answer to all security problems, biometrics is taking off exceptionally slowly in banking environments (Bruno 2001). World wide financial institutions are slowly starting to implement biometrics.

3.4.1 Application areas

The type of biometrics banks should use depends on a variety of factors. Some biometrics, such as retina scanning, is highly accurate. Economically, however, retinal devices are not practical for securing a bank's ATMs, although it may be appropriate to use internally for vault access and

computer networks. A practical mass-market approach to biometrics for banks is devices that rely on existing infrastructure, such as cameras on ATMs (Bruno 2001).

Millions of financial transactions are easily and securely processed using fingerprint technology. A variety of Sagem biometric-based services offer merchants a secure, low-cost payment form that reduces transaction fraud without sacrificing customer convenience (Law Enforcement 2005). Another popular use for banking biometrics is PassVault, made by Diebold. PassVault enables customers to access their safe-deposit box unassisted by bank personnel, by registering their hand or fingerprint scan when applying for a box. Customers enter a PIN and scan their handprint when they want to open the box (Bruce 2001).

An important aspect of biometrics is privacy. To ensure the widespread acceptance and implementation of biometrics, it may be necessary to encrypt the retrieved biometric features. This ensures that someone cannot reconstruct an identifiable fingerprint from an encrypted finger scan stored in the database. Recent incomplete research shows a relationship between personality and the patterns of colours in the iris, igniting a widespread fear that using biometric systems may reveal private information about a person (Patrick 2007).

3.4.2 Advantages and disadvantages

The advantages of biometric systems in the banking environment are numerous, especially for developing countries with newly developing banking networks. These advantages include reducing the surplus of fiduciary money in circulation, and boosts and secures electronic fund transfers and clearing. For many people the most important benefit is ensuring that the right person receives the payment, preventing identity theft and subsequent fraud. Biometric systems also reduce the cost and risk of transporting funds. Developing banking services, and especially encouraging individual savings, can facilitate proper monthly expenditures (Philippe 2004).

Biometrics can be very effective, but is not well suited for users who want to work on multiple machines or in different locations. Many people take work home to do after hours, but without a biometric reader at home, they cannot do their e-commerce transactions (Livewired Communications

2003). Another concern regarding biometrics is their reliability, largely due to media headlines negating the technology in the earliest days of public trials. The most practical disadvantage is the logistics: getting customers to come and register their details (Sturgeon 2005).

3.4.3 Biometric implementations in banks worldwide

Biometric implementation in banks has been successful at the following places:

- Banque Artesia, Amsterdam is using South African company Biometrics.co.za's software to provide banking services to the oil industry in Rotterdam. These high-risk transactions include large sums of money, necessitating an easy to use system that can reliably identify clients before effecting electronic transactions (Burrows 2004).
- The Bank of Tokyo-Mitsubishi, Japan deploys a security system based on vein-pattern recognition at all its branches. The bank's clients use smart Visa credit cards with the customer's vein-pattern information stored on the card's chip to validate their identity when using ATMs (Biometric Technology Today 2004).
- The United States Government Accountability Office reported that the Federal Emergency Management Agency have improperly disbursed more than R7 billion by not validating the identity of aid registrants in the wake of hurricanes Katrina and Rita. One individual received more than R1 million in aid, by registering 13 times using different Social Security numbers (Patrick 2007). ISO published ISO 19092:2008 to increase the security of financial transactions over electronic media. This standard aims to ascertain security requirements for the implementation and management of state-of-the-art biometric identification technology within the financial industry (FindBiometrics 2008c).

3.4.4 Summary

It is crucial that all financial institutions should be as safe as possible. By implementing biometrics worldwide in banks, the country's citizens can rest assured that the economy is safe and stable. A definite boost of confidence in banks is also noticeable. This is due to people who formerly refused to

open bank accounts because there was no foolproof security system in place.

4 BIOMETRICS FOR SENIOR CITIZENS

Senior citizens are generally not up to date with the latest technology trends. However, the use of biometrics in seniors' life can ease many aspects, especially regarding pension allocation.

4.1 Pensioners

According to Joseph Atick, CEO and president of Identix, the public's privacy concerns are a bigger issue than that of cost. He mentioned that senior citizens were more open to biometric technology than the younger generation: they like not having to remember a PIN and want to ensure that their nest eggs are protected (Coogan 2004).

4.1.1 Application areas

Before biometrics made its debut in social welfare, accessing information regarding pension was time consuming and difficult. Senior citizens, who often have difficulty walking, had to go to the appropriate government office and wait in long queues, often in several different offices all over town. Senior citizens can now visit a single biometric kiosk to obtain the relevant information needed to receive pension benefits: databases from the National Institute of Social Security, the National Institute of Employment, the General Treasury of Social Security and the Social Institute for Sea Workers all connect to the system. To use the kiosks, senior citizens have to have a smart card with their name and an ID number, and enrol in the system by scanning either of the index fingers. This ensures that only the enrolled person can receive monetary benefits from the system. In cases of frailty or illness, the system can fingerprint a family member or friend to collect the allowance on behalf of the beneficiary (Gemplus Corporation 2002). The system is also adapted to allow for payment of pensions via ATMs. Using these ATMs, pensioners can access their cash at any time, at the touch of a finger. They now do not need to carry large amounts of cash with them anymore and make them less vulnerable to thievery when travelling home (FindBiometrics 2004).

Before the implementation of the biometric system, it was easy to obtain pension benefits illegally. If someone lost their ID card, an

unauthorised individual could use it to access the cardholder's medical records or pension benefits. The best way to protect against these types of incidents is to combine verification of both the card and the fingerprint (Pronko 1998).

The ideal biometric system to implement for social welfare would involve digitised photographs and hand geometry stored in a central database. A plastic identity card with a magnetic strip will contain the photograph, the client's analogue signature and date of birth, a selection of security features and a thumbprint. Authorised staff members at multiple sites will use data scanned from a person's hand to search the databank for matches and interface with the existing information systems (Davies 1994).

4.1.2 Advantages and disadvantages

The most outstanding benefits of biometric applications regarding social welfare industries are that pensioners receive their benefits in a faster, more convenient and secure way. The synergistic effect of offering welfare and pension payments through biometrics-equipped bank ATM networks offer many benefits. Government can reduce its cost and provide a more efficient and timely service to its constituents; financial institutions can increase the volume of transactions, whilst reducing the unit transaction costs; banks' cumulative revenues can be increased by charging the government agencies for the service. Hopefully, in the long run the public at large can benefit from reduced taxes as a result of a more efficient government (Yanez & Gomez 2004).

By implementing these social assistance cards with smart card technology, the biometric system adds inherent security features. The decent storage capability and the electronically readable format make the smart card the optimal solution to address the social welfare program's major security, financial control and portability concerns (Gemplus Corporation 2002). Disadvantages include that only government agencies may do capturing and storage of fingerprints for it to be considered legal (Yanez & Gomez 2004).

4.1.3 Biometric implementations regarding pension distribution worldwide

- Spain's government incorporated biometric verification units with information kiosks to allow citizens to access personal information, pension and healthcare benefits. The 633 kiosks are located in different government offices in the Andalusia region of Spain, and will eventually be implemented nationwide (Pronko 1998).
- South Africa's government has had difficulty with the payout of pensions to the elderly, especially those in remote areas who often have limited mobility. In 2001, the government started doing pension payments through a mobile van distribution pay points as part of their plan to bring the government services closer to the people. HighTech Laboratories designed the system to use about 500 vans, fitted with ATM-style machines and Identix BioTouch USB fingerprint readers (Identix 2004).
- The Philippine Social Security System launched an identification card system in November 1998 to ensure that members, pensioners and dependants do not enrol using multiple identities (Breedt & Olivier 2004).

4.1.4 Summary

By introducing biometrics in the area of pension retrieving, the lives of the senior citizens become less complicated. The adoption of such implementations has been slow, but it has proved to be successful.

5 CONCLUSION

In No age discrimination for biometrics, we showed that biometrics applies to all facets of human life. The research focused on three distinct age genres, reviewing each area, as well as both successful and unsuccessful implementations. Many of the applications discussed under adult biometrics are applicable to both the younger and older generation, but falls favour to the most prominent category. For example, while children from primary school level upwards use a savings account, and retired people often put their pension in a bank account, usually adults make the most noteworthy financial decisions.

After examining the school environment, the immigration and healthcare industries, law enforcement, the banking environment and pension distribution, it is clear that the advantages far outweigh the disadvantages of using biometrics for security. The common advantages include increased security, reduced fraud, less administration problems created by forgotten passwords, easier employee auditing and logging and significant cost savings (QuestBiometrics 2005). In most cases, the most prominent disadvantage is user resistance, which will significantly lessen as the technology becomes more widely accepted.

6 REFERENCES

AB. 2006. A Short History of Biometrics. Associated Content -The People's Media Company. [Available from: http://www.associatedcontent.com/article/48809/a_short_history_of_biometrics.html (Accessed 7 February 2008)].

Arnold, B. 2006. Caslon Analytics biometrics. [Available from: http://www.caslon.com.au/ biometricsnote1.htm (Accessed 7 February 2008)].

Beckley, A. 2004. The Future of Privacy in Law Enforcement. FBI Law Enforcement Bulletin. [Available from: www.accessmylibrary.com/coms2/summary_0286-31073479_ITM (Accessed 15 August 2005)].

Beyond doors: Securing records with finger flick. 2002. Security, 39(7):57. [Available from http://0-proquest.umi.com.raulib.rau.ac.za:80/pqdweb?did=181577441&sid=7&Fmt=4&clientId= 57200&RQT=309&VName=PQD (Accessed 10 August 2005)].

Biometric Technology Today. 2004. US -Visit awards fingerprint services contract. Biometric Technology Today, 12(10):5.

Biometric Technology Today. 2005. Passport plans in disarray. Biometric Technology Today, 13(5):2.

BIOMETRICS in Education. [Available from: http://webhost.bridgew.edu/jcolby/it525 (Accessed 10 August 2005)].

Borja, R. 2002. Finger-Scanning Technology Monitors School Employees. [Available from: http://www.edweek.org/login.html?source=http%3A%2F%2Fwww.google.co.za%2Fsearch%3Fhl%3D af%26q%3D%2522Finger-Scanning%2BTechnology%2BMonitors%2BSchool%2BEmployees%2522%2BBorja%26meta%3D&destination=http%3A%2F%2Fwww.edweek.org%2Few%2Farticles%2F2002%2F10%2F23%2F08biometric.h22.html&levelId=2100&baddebt=false (Accessed 15 April 2008)].

Breedt, M. & Olivier, M. 2004. Using a central data repository for biometric authentication in passport systems. [Available from: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/072.pdf (Accessed 12 February 2008)].

Bruce, L. 2001. Face-scanning, fingerprinting ATMs gain ground. [Available from: http://www.bankrate.com/brm/news/atm/20010302a.asp (Accessed 10 April 2008)].

Bruno, M. 2001. Biometrics Are Too Hot to Handle. [Available from: http://www.encyclopedia.com/ doc/1O8-biometrics.html (Accessed 12 February 2008)].

Business Wire. 2008. US Biometrics Corporation to Conduct The First In Its Series of Biometrics Education Seminars to Universities and Colleges Across The United States. [Available from: http://www.pr-inside.com/us-biometrics-corporation-to-conduct-the-r427644.htm (Accessed 8 February 2008)].

Burrows, T. 2004. Dutch bank using SA biometrics. [Available from: http://www.itweb.co.za/office/ grintek/0308010725.htm (Accessed 10 August 2005)].

Coogan, J. 2004. FACT Act Provision Raises Biometrics' Profile. American Banker. [Available from: http://www.biometricgroup.com/in_the_news/03_17_04.html (Accessed 13 February 2008)].

Dalton, A. 2004. Eye Spy. Hospitals & Health Networks. 78(11):12. [Available from http://0¬proquest.umi.com.raulib.rau.ac.za:80/pqdweb?did=750586381&sid

=6&Fmt=4&clientId=57200&R QT =309&VName=PQD (Accessed 21 August 2005)].

Davies, S. 1994. Touching Big Brother: How biometric technology will fuse flesh and machine. [Available from: http://www.asylumsupport.info/publications/privacy/biometrictechnology.htm (Accessed 13 April 2008)].

FindBiometrics. 2003. BIO-key Scores Straight A's in Education Application. FindBiometrics.com.[Available from: http://www.findbiometrics.com/viewnews.php?id=512 (Accessed 10 March 2008)].

FindBiometrics. 2004. NCR and Bancafe Use Biometric Technology to Reach New Colombian Banking Customers. [Available from: http://www.findbiometrics.com/press-release/1795 (Accessed 12 February 2008)].

FindBiometrics. 2008a. AuthenTec Reports Record Fourth Quarter 2007 Financial Results. [Available from: http://www.findbiometrics.com/press-release/4886 (Accessed 8 February 2008)].

FindBiometrics. 2008b. Case Study: Iris Recognition Enhances Security, Accelerates Traffic, and Reduces Costs at Border Crossing. [Available from: http://www.findbiometrics.com/Pages/ airport_articles/lg-case-study.html (Accessed 8 February 2008)].

FindBiometrics. 2008c. Safer electronic financial transactions with new ISO standard for state-of¬the-art biometric authentication. [Available from: http://www.findbiometrics.com/press-release/4896 (Accessed 8 February 2008)].

FindBiometrics. 2008d. New Russian Biometric Passports With Empty Chips Issued. [Available from: http://www.findbiometrics.com/article/495 (Accessed 8 February 2008)].

Gemplus Corporation. 2002. Aplitec Social Assistance and Pension Card. [Available from: http://www.gemalto.com (Accessed 18 February 2008)].

Goldberg, L. 2003. Creating Safer and More Efficient Schools with Biometric Technologies. [Available from: http://www. thejournal.com/articles/16433 (Accessed 10 March 2008)].

Graham-Rowe, D. 2005. Ear biometrics may beat face recognition. [Available from: http://www.newscientist.com/article.ns?id=dn7672&feedId=online-news_rss20 (Accessed 2 March 2008)].

Graziano, C. 2003. Learning to Live With Biometrics. [Available from: www.wired.com/ news/privacy/0,1848,60342,00.html (Accessed 10 March 2008)].

Hudson, A. 2003. Tampa cops end camera program. The Washington Times. [Available from: http://0-search.epnet.com.raulib.rau.ac.za/login.aspx?direct=true&db=nfh&an=4KB20030821094511 (Accessed 15 August 2005)].

Identix. 2004. South African National Pension Payout Program: Facilitating Entitlement Distribution. [Available from: http://www.ibia.org/membersadmin/casestudy/pdf/9/South%20Africa%20National%20Pension.pdf (Accessed 12 February 2008)].

ITWeb. 2006. Jo'burg utilises biometrics. [Available from: http://www.itweb.co.za/sections/computing/2006/0608301030.asp?S=Biometrics&A=BIO&O=FRGN (Accessed 8 February 2008)].

Johnson & Wales University. 2002. Denver is First University in Colorado to Utilize Biometrics to Gain Access to Dorm Rooms. 2002. [Available from: http://www.jwu.edu/media/pressarc/ 02/co11_21_02.htm (Accessed 10 March 2008)].

Kennard, L. 2002. SCANNING STUDENTS: A Stockholm School Goes Biometric. [Available from: http://support.novell.com/techcenter/articles/nc2002_05b.html (Accessed 11 February 2008)

Law Enforcement. 2005. [Available from: http://www.morpho.com/company/our_markets.html (Accessed 3 December 2007)].

Livewired Communications. 2003. [Available from: http://www.itweb.co.za/office/grintek/ 0308010725.htm (Accessed 10 August 2005)].

Mansfield, S. 2003. Password Proliferation Alleviated. Security, 40(9):39-40. [Available from: www.accessmylibrary.com/coms2/summary_0286-31104683_ITM (Accessed 15 March 2008)].

from: www.networkworld.com/news/2004/121304biometrics.html (Accessed 17 March 2008)].

Nixon, S. 2003. School roll could be replaced with eye scan. [Available from: www.smh.com.au/ articles/2003/03/07/1046826531945.html (Accessed 10 March 2008)].

Out-Law News. 2004. Debunking six myths of biometrics. Out-Law.com. Out-Law News, 09/07/2004. [Available from: http://www.out-law.com/ page-4698 (Accessed 12 February 2008)].

Patrick, A. 2007. Biometrics and Identity Theft. [Available from: http://www.andrewpatrick.ca/ essays/biometrics-and-identity-theft (Accessed 7 February 2008)].

Philippe, H. 2004. SAGEM provides the first biometric system to secure a major banking application. [Available from: www.sagem-ds.com/eng/site.php?spage=03010419 (Accessed 26 March 2008)].

Pronko, N. 1998. Biometrics Protects Government Data. Business Solutions. [Available from: http://www.businesssolutionsmag.com/index.php?option=com_jambozine&layout=article&view=p age&aid=2277&Itemid=5 (Accessed 13 March 2008)].

QuestBiometrics. 2005. Advantages of Biometrics: Why opt for biometric technology? [Available from: http://www.questbiometrics.com/advantages-of-biometrics.html (Accessed 7 February 2008)].

Reynolds, P. 2004. The Keys to Identity. Health Management Technology, 25(12):12-16. [Available from: www.healthmgttech.com/archives/1204/1204the_keys.htm (Accessed 5 February 2008)].

Schneider, J. K. 2005. National health infrastructure prompts need for proper patient identification. Managed Healthcare Executive, 15(8):22-24. Available from: http://managedhealthcareexecutive.

modernmedicine.com/mhe/Hospitals+&+Providers/National-health-infrastructure-prompts-need-for¬pr/ArticleStandard/Article/detail/173306 (Accessed 20 March 2008).

SearchSecurity.com. 2006. Biometrics. [Available from: http://searchsecurity.techtarget.com/ sDefinition/ 0,,sid14_gci211666,00.html (Accessed 7 February 2008)].

Security International. 2002. City of Stockholm School System. Precise Biometrics. [Available from: http://www.security-int.com/categories/fingerprint-identification/city-stockholm-school¬system.asp (Accessed 12 February 2008)].

Sturgeon, W. 2005. 'We want biometrics' say bank customers. [Available from: http://software. silicon.com/security/0,39024655,39130185,00.htm (Accessed 9 April 2008)].

US Department of State. 2004. DoS awards record breaking biometric deal. 2004. Biometric Technology Today, 12(10):1,12.

Wikipedia. 2008a. Fingerprint. [Available from: http://en.wikipedia.org/wiki/Fingerprint# Timeline (Accessed 8 February 2008)].

Wikipedia. 2008b. Ted Bundy. [Available from: http://en.wikipedia.org/wiki/Ted_Bundy (Accessed 8 February 2008)].

Wikipedia. 2008c. Forensic dentistry. [Available from: http://en.wikipedia.org/wiki/Forensic_ dentistry (Accessed 8 February 2008)].

Wikipedia. 2008d. Biometric passport. [Available from: http://en.wikipedia.org/wiki/Biometric_ passport (Accessed 8 February 2008)].

Winton, R. 2004. ID System Gets in Face of Criminals. [Available from: http://pqasb.pqarchiver.com/ latimes/access/770653801.html?dids=770653801:770653801&FMT=ABS&FMTS=ABS:FT&type =current&date=Dec+25%2C+2004&author=Richard+Winton&pub=Los+Angeles+Times&edition= &startpage=B.1&desc=ID+System+Gets+in+Face+of+Criminals%3B+LAP

D+officers+field-test+a+ hand-+held+computer+using+facial+recognition+to+identify+suspects.+Critics+raise+issues+of +privacy+and+reliability (Accessed 12 February 2008).

Yanez, M. & Gomez, A. 2004. ATM & BIOMETRICS: A SOCIO-TECHNICAL BUSINESS MODEL. P7 – 9. University of Miami, School of Business Administration.

Zalud, B. 2003. Facial Makeover. Security, 40:30-32.