IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP5246

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour. Copyright 2005, Idea Group Inc.

Ethical Issues Associated with Biometric Technologies

Mensur Cehic and Marian Quigley
School of Multimedia Systems, Monash University, Clyde Rd., Berwick,
Victoria, Australia, 3806, marian.quigley@infotech.monash.edu.au

ABSTRACT

This paper examines the benefits and ethical dilemmas associated with the implementation of biometric technologies for security purposes. Generally regarded as a highly accurate and effective means of controlling access to areas of high security, the technology still contains flaws and allows a small but significant margin of error. At a time when governments and organisations are calling for stringent measures to combat threats of global terrorism and the increasing incidences of identity fraud, members of the general public are expressing genuine concern at what they perceive as the threat to individual privacy posed by the increased use of surveillance and identification technologies. The paper argues that a revision of existing laws along with the establishment of a sound ethical framework should take precedence. In particular, the paper addresses the necessary abolishment of ambiguity issues surrounding biometric data with reference to definitions of personal/sensitive data. Such a process would allay public concerns and enable the acceptance and successful implementation of this innovative technology.

INTRODUCTION

Biometric technology involves effective methods of individual identification/authentication through its recognition of unique physiological characteristics. Although still a developing technology which contains deficiencies, it is generally considered to be a highly accurate and widely applicable security measure. Biometric technology has experienced an enormous upsurge in demand, research and development due to the recent increases in threats of global terrorism and cases of fraud and identity theft. However, growing public awareness of this technology has been accompanied by increasing concerns about ethical issues associated with its use.

BIOMETRIC TECHNOLOGY

Identification and authentication involve a three-step process:

1. Attainment of physiological characteristics by means of an image scan or sound sample
2. Templating of extracted minutiae data (attributes) from scanned image
3. Matching template with stored data

In cases where an additional token is used, such as a passport, the same process is applied to match the template with data stored in the chip containing an individual's biometric data.

The three-step process involves one or a combination of the following techniques:

- Fingerprinting
- Face Recognition
- Iris Scanning
- Voice Recognition
- Hand Geometry

Benefits of Biometric Technology

Biometrics guarantees a high level of accuracy in the identification of individuals thereby enabling control of access to secured areas such as investment banks, research labs, educational institutions, government buildings, customs points and airports.

According to Ohlhorst (2004), the so-called identity management market has enormous potential for growth, with expectations exceeding US $3.3 billion within the next couple of years in the United States alone. Biometric technologies are likely to have a significant role in this booming industry.

Integration with Other Technologies

After the 9/11 terrorist attacks in the USA, many governments began utilising biometric technologies – at least as trial runs. With surveillance measures already in full steam across Britain and other European countries, and especially within the densely populated, technologically advanced nations in South East Asia, the potential of certain biometric techniques is amplified by their integration with new and existing technologies such as biometric IDs and centralised databases.

Banking, Airport Security and Access Control

Biometrics can contribute significantly to lowering administrative costs whilst bolstering security through unique access control methods. According to Price-Waterhouse-Coopers, 20 percent of larger British corporations suffered security breaches in 2003 because of inadequate access control. Moreover, only 6 percent of these British companies had some biometric technology in place. Further studies undertaken by Price-Waterhouse-Coopers found that early adopters of such technologies have had significant reductions in security and related incidents.

A growing number of U.S. banks are now moving towards biometric access control. The Bank of America plans to establish 500 new banking centres across the United States by 2005 – all of which will be biometrically secured mainly through hand geometry scanning. This is to be enforced for services such as ATMs and access to vaults. According to Krebsbach (2003, p.2), the main driving force towards biometrics in this sector is the need to reduce identity theft that now costs up to US$5 billion per year. In 1999-2000, Bank United conducted its first biometrics pilot run at three of its 150 ATMs in Texas where up to 700 customers participated. According to a report published in *American Banker* (1999, p.14), it produced a 98 percent approval rating from customers who commended the effectiveness of the identification/authentication methods used.

It is no secret that biometrics have great security potential and proven accuracy. Many airports with biometric identification/authentication systems currently possess only basic capabilities, but this has been changing rapidly since 9/11. In recent years, the U.S. in particular, has seen an increased introduction of biometrics at airports. Other countries, including Germany and Britain are following suit.

Levels of Public Acceptance

Although public tolerance levels of biometrics vary from country to country, a US study shows that 87% of Americans consider fingerprinting to be a legitimate identification requirement; 91% believe the use of fingerprint scanning is justified to control access to high-security areas, whilst approximately 76-77% believe it should be used for identification in personal finance procedures such as cashing personal cheques for large amounts or credit card use (http://www.ipc.on.ca/).

The socially acceptable forms of biometric technology tend to be those that are voluntary and non-intrusive. For example, biometric systems with databases holding data about registered e-passport holders as well as criminals, terrorists and suspects belong in this category. Similarly, within the business realm, systems would entail biometric data of persons who have obtained authorization to access any types of inter-organizational processes (stock exchange, transfer of funds, logistics, etc.) or access to their own financial records (eg. ATMs). This, too, is a rather limited manipulation of data that is easily protected and has a very low potential of privacy intrusion. Other acceptable uses are those relating to restricted area access control whereby biometric systems simply ensure authorised entry to sensitive sectors within a nation's infrastructure such as airports.

The form of biometric technology which causes most public concern, however, is national biometric-enabled ID cards because they would be mandatory and also open to unprecedented surveillance. Unlike electronic passports, which help prevent unwanted individuals from entering a country, national biometric ID cards would abolish anonymity and could easily be misused. The regulation of access to collected data would be extremely difficult given the current lack of biometric focus within privacy legislation. Moreover, the collection would be frequent and very intrusive and could be misused for commercial and other purposes rather than for law enforcement and national security. As Crews (2003, p.16) explains, widespread surveillance, such as that utilising national biometric ID cards, would undermine the very purpose of biometric implementation in terms of national security and moreover, it would become a general law enforcement tool which would have little to do with combating terrorism.

According to the Australian Federal Privacy Commissioner, Malcolm Crompton, many possible biometric threats to privacy are associated with *how* biometric systems are used and *which* biometric attributes are collected (Crompton, 2002, p.4).

For example, fingerprinting is predominantly accepted within societies, unlike DNA sampling which can be unfairly used for discrimination (for example, declining insurance services to customers prone to illness). In most cases, biometric technology is widely accepted due to its effectiveness. However, without rigorous standards and regulation, the information collected could be used improperly.

It is precisely this lack of standards and regulations that is posing a direct danger to privacy. The infamous USA Patriot Act – an Act which was signed into law some 40 days after 9/11 for the purpose of better responding to such threats as terrorism and identity fraud – has narrowed the gap between justified surveillance and the establishment of a digitally policed state.

Mistrust of Governments

The importance given to the protection of an individual's privacy in many Western nations underlies their citizens' suspicion of significant change in the use of identification/authentication methods and public awareness of their potential for abuse. In the U.S., the value of privacy has been highlighted at a time when the government is trying to protect citizens from further terrorist attacks. For example, a number of U.S. citizens voiced their outrage regarding the Patriot Act because of its wider than necessary reach into citizens' privacy. This sentiment is best described by the Electronic Frontier Foundation's (http://www.eff.org/Privacy/Surveillance/Terrorism) USA Patriot Act Analysis page:

> *We have given sweeping new powers to both domestic law enforcement and international intelligence agencies and have eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused.*

In another example, Timothy Edgar – a prominent ACLU attorney – states that the US-VISIT program is a privacy infringement waiting to happen since the biometric records obtained from foreigners are likely to be kept after they become U.S. citizens and could potentially be shared with foreign governments.

There is also a growing belief that biometric technologies provide a false sense of security and that they involve a direct infringement on privacy for the sake of limited improvements to security. As noted by Guterl et al, "many security experts have questioned whether the surveillance machinery that nations have been erecting since 9/11 is as effective in dealing with the threat from terrorist groups like Al-Qaeda as most people believe". They also argue that the "ritual" of biometric authentication/identification at airports and frequent encounters with cameras in other sensitive public places may "make people feel safer" but do not necessarily provide genuine protection although they intrude on individual privacy (2004, p.2).

The Potential for Misuse

The human body offers much more data than is required for authentication/identification purposes. For instance, some systems installed at airports include a body/face temperature check. So far, this has mainly been used to control or prevent SARS epidemics. The possibility of excessive collection of physiological data is linked to the possibility of unfair discrimination against members of the public. For example, if such technologies were used in commercial realms and an insurance company began checking its potential customers' health through information obtained by an integrated biometric system, persons seeking service could be discriminated against. As camera surveillance is becoming commonplace in societies around the world, the possible unregulated increase of biometric authentication/identification nodes within an individual's daily life could also provoke extreme marketing by commercial enterprises.

Although this evokes science-fiction scenarios such as *Minority Report*, it is true to say that societies are indeed creating the frameworks for such a surveillance environment and, considering all the benefits of biometrics - when used appropriately - its use is likely to increase. It is therefore necessary to establish ethical guidelines that ensure the efficient provision of security whilst maintaining individual freedom and privacy.

Preventing Misuse

Although it is important to note that most privacy advocates seem to focus on the potential abuse of biometric technologies rather than their benefits, the establishment of legal/ethical frameworks and standards for the safe storage and protection of an individual's biometric data is imperative. In order to achieve this, legislation must be updated.

In Australia, the Privacy Act 1988 does not fully cover all potential applications of biometric systems. Furthermore, there are differences in opinion as to whether biometrics fully qualify as personal information. In Britain, on the other hand, most law firms consider biometric data to belong under existing privacy and data protection legislation and some even advise strict attention to information security. According to Pritchard (2004, p.6), because biometric data cannot be changed, any misuse or compromise of that data could present serious consequences for an individual in the future: for instance, stealing fingerprint data in order to falsify a print and leaving it at a crime scene can place unnecessary scrutiny on an innocent individual.

This calls for legislative clrity regarding individuals' biometric data. As with the Australian Privacy Act, the lack of specific wording and the failure to classify biometric data as private/personal could have adverse effects in the future. For instance, the Act defines personal information as:

Information or opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The closest reference to biometric data here is the word “recorded”. The Act does not specify biometric data – at least not directly. It specifies: document, database (however kept), photograph or other pictorial representation of a person. Both “document” and “database” would have to contain sensitive information to be considered personal. This leaves us with “photograph”. The closest biometric technique here would be facial recognition, which initially involves photographs but ends up as raw data (e.g. barcode). Hence, the raw data – which only includes a coded representation of the unique features of a face but not an actual photograph – is used for matching in the identification/authentication processes. Consequently, biometric data does not fall into the sensitive information category. Even Crompton (2002) emphasises that biometric data does not currently qualify as sensitive information but has the ability to reveal sensitive information.

However, if common sense prevailed, biometric data would have to be at the top of the list of sensitive information types since data derived from individuals’ unique – and irreplaceable – physiological characteristics is nothing but personal. This argument can be further supported from a slightly more technical perspective. In database management terms, if the (biometrically derived) raw data uniquely identifies an individual then it has the potential of a primary key (unique identifier). Under any other circumstance, a record could have a new primary key assigned (for example, even a tax file number can be replaced), whereas the biometric unique identifier as a primary key is irreplaceable. Thus, one can’t affix a new iris, fingerprint, etc. Furthermore, biometric data obviously acts as the primary key that can reveal other sensitive information. In fact, this is a good reason biometric data should not only be deemed as sensitive information but as the ultimate personal information. No other sensitive data has this ability to uncover all other personal details about the particular individual. In fact, biometric data can be used to accumulate all additional information since it has the potential to become the ultimate tracking technology – given more widely spread scanning nodes (surveillance cameras, biometric ATMs, airports, etc.). In contrast, one’s personal political opinions, sexual preferences or philosophical beliefs are not mutually revealing.

Ambiguities, Flaws and Lack of Awareness

In other cases, existing laws regulating biometric data usage, storage and collection are quite ambiguous. One of the most notable examples is the Quebec Act to Establish a Legal Framework for Information Technology (Rola, 2002). This particular law has been in effect in Canada since late 2001, but most of Quebec’s companies knew little of the details regarding the protection of privacy. Whilst these organizations were seeking more information about what exactly this legislation entailed, some relevant government departments had trouble providing it as they were confused by it themselves. This was simply because the law did not outline the steps required to protect personal information – including biometric information.

Addressing the issues of potential abuse and its impact on privacy through *thorough* – and above all – *early* standardisation and regulation ensures socially harmless and effective implementation on a national and global level. This is best emphasised by the Electronic Privacy Information Centre, which states: “Often the problem is that invasive surveillance technologies are rolled out before the policy debate concerning the guidelines for the use of these systems.” (http://www.odpp.nsw.gov.au/speeches/FingerprintsConferencePaper.htm)

Tracking, Loss of Individual Anonymity and Control

The American Civil Liberties Union sees the introduction of biometrics as a means of tracking individuals for purposes unrelated to combating threats to American society.

Many critics argue that without a thorough scrutiny of the use of biometric databases, the possibility of tracking is imminent. Many commonplace surveillance capabilities in societies can – and are already – utilised for locating and tracking individuals for law enforcement purposes, but biometrics provides much greater accuracy. Recently, the Electronic Frontier Foundation outlined the major pitfalls and side effects that could arise should biometric systems not be covered by precise legislation. These are:

- Increased visibility of individual behaviour – lack of anonymity
- Matching people’s behaviours with predetermined patterns – intrusive micro-marketing
- Empowerment of corporations at the expense of privacy
- Personally and politically damaging disclosures – elimination of competition in public service (http://www.eff.org/privacy/surveillance/biometrics.php).

CONCLUSION

A greater insight into the current limitations and vagaries of existing laws can help to more fully safeguard privacy. Wider-reaching and ethical implementation of biometric technology is possible, but this is dependent upon public trust. It is only possible if appropriate reviews and/or amendments of national Privacy Acts are carried out. Currently, it can be concluded that the main obstacle to proper privacy protection within the biometric realm is the definition of personal information. Biometric data is derived from individuals’ physiological characteristics which are unique, irreplaceable and personal.

Countries such as Australia and the U.S. need to amend their existing privacy laws. These amendments must clearly include biometric data under the definition of personal/private/sensitive information and access to this must be appropriately protected and the protection monitored. Although certain voluntary, non-intrusive biometric technologies have received public acceptance, this acceptance should not be taken for granted. In the U.S., there is growing concern that biometrics provide a false sense of security whilst the Patriot Act has increased citizens’ mistrust of government. The slightest breach of privacy or encroachment of individual liberty could easily prevent public acceptance of biometrics. This would be most unfortunate given the societal benefits these technologies offer. Threats to privacy are related to how biometrics is used and which attributes are collected. Consequently, specific federal guidelines/standards must be introduced to ensure that the data that is collected is limited to that specified – so that, for instance, fingerprints are not taken when only an individual’s hand geometry is required. In addition, the storage of this data must be legally protected. Only by implementing the aforementioned changes and standards can societies enjoy the benefits of biometrics without any amelioration of civil liberties and individual privacy.

REFERENCES

Crews, C. W., 2003, ‘Monitoring Biometric Technologies in a Free Society’, *USA Today,* vol. 132, iss. 2698. New York.

Crompton, M., (2002), Biometrics and Privacy – The End of the World as We Know It or the White Knight of Privacy? *Biometrics Institute Conference*, Sydney.

Electronic Frontier Foundation (2004 – copyright). Censorship & Privacy – Terrorism Archive [Censorship & Privacy – Terrorism Archive], [Online]. Available: http://www.eff.org/Privacy/Surveillance/Terrorism [2004, June 02]

Guterl, F. et al, 2004, ‘Taking a Closer Look; Governments the World Over Are Watching Citizens Like Never Before. But Are We Any Safer For It?’

IPC (2004 – copyright). IPC Publications and Presentations [Publications and Presentations], [Online]. Available: http://www.ipc.on.ca/ [2004, June 05]

Krebsbach, K., 2003, ‘SECURITY: Biometrics Takes Hold Overseas; Significant Hurdles Remain to Adoption in the U.S.’, *Bank Technology News*, vol. 16, iss. 12, New York.

Office of the Director of Public Prosecutions (2004 – copyright). Fingerprints Conference [Fingerprints Conference], [Online]. Available: http://www.odpp.nsw.gov.au/speeches/Fingerprints ConferencePaper.htm [2004, June 02]

Ohlhorst, F.J., 2004, 'VARs Can Help Solve the Identity Crisis', *CRN*, April 12, vol. 22, is. 1091, Jericho.

Price Waterhouse Coopers (2004 – copyright). Publications [Publications], [Online]. Available: http://www.pwc.com/extweb/pwcpublications.nsf [2004, April 20]

Pritchard, S., 2004, 'Security Now a Fact of Business Life', *The Financial Times*, vol.18, iss. 10, London.

Rola, M., 2002, 'Quebec Mystified by e-biz legislation', *Computing Canada*, 28 (18), Willowdale.