Biometric Implementations and the Implications for Security and Privacy

Vassiliki Andronikou[1], Dionysios S. Demetis[2] and Theodora Varvarigou[3]

[1,3] National Technical University of Athens
Department of Electrical and Computer Engineering
9 Heroon Polytechniou Str., Zografou 15773, Athens, GREECE

[2] London School of Economics and Political Science
Department of Management – Information Systems and Innovation Group,
Houghton Street, WC2A 2AE, London, UK

Abstract

Biometric technologies such as fingerprint, face and iris recognition have seen an increasing interest throughout the past decades. Such interest has been intensified with various large-scale initiatives from governments that seek to incorporate biometric technologies for the purposes of identification and verification. Far from being purely ad hoc technological implementations, biometric devices are now seen as being of strategic value and consequently of strategic importance. With the perception of better efficiency and effectiveness, governments are beginning to embrace biometric technologies. Industry is also geared up to sell the products, and all over the world businesses are looking to incorporate biometrics for many different uses ranging from access-control to e-commerce and entertainment. This paper seeks to review the crucial security and privacy issues that affect such biometric implementations and point towards aspects which should be considered for the prudent management of Information Systems that utilise biometric technological components.

Introduction

Biometric technologies have been the source of much debate lately as governments have outlined their long term vested interests in them by proposing large scale implementations, such as biometric passports. Such interest from government has been reinforced by increasing commercial interest. As biometrics are intrinsically related to identification and authorization, security and privacy concerns become unavoidable. Inadequate handling of either aspect can severely jeopardize biometric data which are tightly linked with personal identity. Following a brief introduction to biometrics, we shall – in our analysis – review the related security and privacy concerns pertaining to biometric implementations.

The term *biometrics* comes from the combination of the Greek words ‘bios’, which means life, and ‘metrikos’, which in its turn means measuring. Biometric technologies aim primarily at identifying a person’s unique features, be those physiological or behavioural. While *physiological (or passive)* biometrics refer to fixed or stable human characteristics, *behavioural (or active)* biometrics measure characteristics represented by skills or functions performed by an individual. Examples of physiological biometrics are fingerprints, iris patterns, hand geometry, DNA and facial image, while signatures, keystroke dynamics and mouse movements belong to behavioural biometrics (FIDIS 2005).

Two general uses of biometrics are *identification* and *verification* which both require the existence of reference data that the person’s measured traits will be compared with reference templates or raw data. During these processes, a biometric data sample is compared against the respective biometric data of every person enrolled in the database or against a single reference template of a particular enrolled individual in order to confirm the identity of that person respectively. When a biometric system correctly identifies a person, then the result of the identification process is a *true positive*, whereas if the system correctly rejects a person as not matching the respective enrolled template, the result is a *true negative*. Similarly, when the system incorrectly identifies or rejects a person then we speak about a *false positive* or a *false negative,* the security aspects of which will be discussed in a subsequent section.

Security in Biometric Implementations

Implementations that involve a biometric component in the process of identification are highly prone to security risks - much more so than for simple verification tasks, as we analyse in the following section. With governments planning to adopt biometrics, biometric technologies are inscribed with a strategic value. The strategic value in biometric implementations not only stems from long term government plans but also from the unique and critical function that biometric technologies embody. Some governments also express their long-term commitment to biometrics and go beyond their own identification-supported processes, suggesting use of their databases by various industry stakeholders (i.e. financial institutions). For example, the UK government envisions that industry stakeholders will be able to verify their customers' identities by connecting to the government databases before allowing them to use their own services (LSE 2005).

Such implementations and the complex infrastructures that become biometrically supported at both national and international levels are therefore creating truly strategic information systems and elevate the importance of the biometric components; biometric technologies in this context are much more than a simple technological artefact.

Taken the projected importance of those technological applications that attempt to resolve the issue of identification by including a biometric component, it is crucial to highlight the major security aspects that surround such a domain. Far from being a purely technical matter, we will treat the issue of security in biometric implementations as being heavily influenced by the context of implementation, and hence, factor additional aspects into our considerations. While we start with a description of somewhat technical issues around the domain of biometric security, we acknowledge that Information Systems (IS) security is much broader. Beyond the purely technical aspects that have to be considered, there are also formal aspects that relate to IS security (i.e. policies and processes) but also informal and more subtle aspects that can influence the security of a biometric implementation (i.e. cultural norms). The latter requires that additional principles have to be considered for the management of IS security regarding biometric implementations; responsibility, integrity, trust and ethics will have to be present for enhancing security, either within governments or organizations (Dhillon and Backhouse 2000).

In the following section, our analysis will focus on the security breaches of biometric systems in the context of their broader infrastructure and not the different biometric techniques used, such as iris or fingerprint. One of the most common misconceptions that relates to biometric security sees most of the security vulnerabilities in the biometric reader device itself or in the template created by the biometric data. While it is true that the biometric reader and the template remain the obvious points of attack, the security issues are much more complex, with researchers demonstrating eight points that are prone to attack (Uludag and Jain 2004). These are portrayed in the following figure and described briefly below.

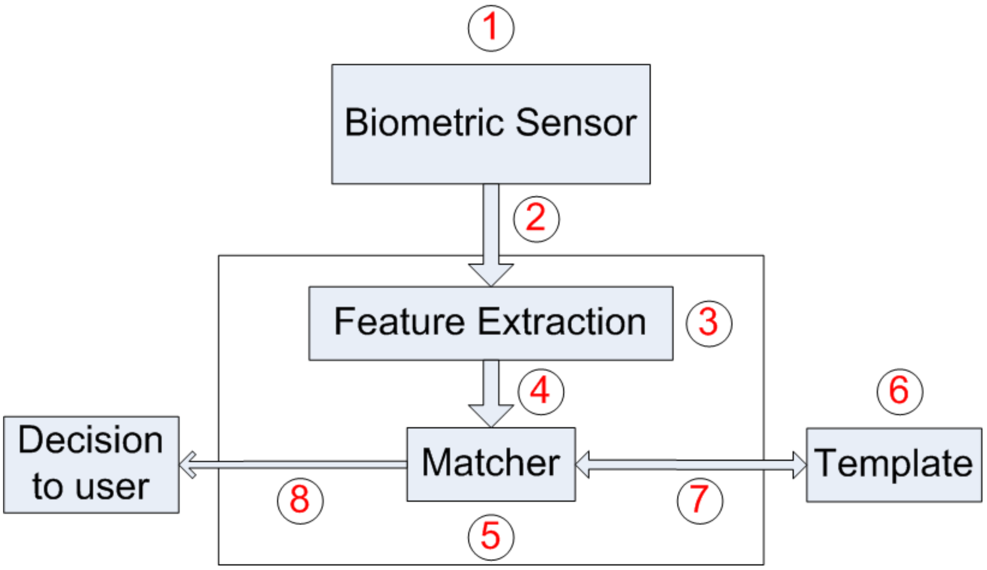

Figure 1. *Adapted version of the original on the attack points of a biometric implementation (ibid)*

As user-system interaction takes place via the biometric sensor, attacking the device that captures the biometric becomes the first obvious point of attack. Systems that can imitate biometrics have successfully been used for this purpose while instructions on how to create prosthetic fingers can already be found on the internet[1]. The success of attacks using prosthetic fingers is crucial from a security standpoint; researchers from Japan have demonstrated a success rate in attacks on such biometric devices in the range of 67-100% (Matsumoto, Matsumoto et al. 2002). The major factor that determines the success rate of the attacks was found to be the quality of the original print (ibid). There are of course some biometric systems that can be enriched by incorporating aliveness detection methods but those cost significantly more while most current commercially available aliveness tests can be easily cheated (FIDIS 2005).

Besides the direct attacks and the device itself, there are other Points of Attack (PA) worth a brief overview. As the biometric device receives information from the submitted biometric (i.e. fingerprint) and converts it to data, it is possible that to replay that data to gain authorization to the system, something that constitutes PA 2. In PA 3, the feature module can be forced to produce different values than those generated from the sensor input. In PA 4, unauthorized access may be gained by replacing the system generated values with known ones, while in PA 5, the matcher can be forced to produce a high or low matching score where the attacker can simulate a false positive or negative respectively

The last three points of attack of a biometric system present considerable security challenges. Despite the fact that the template is one of the cliché points of attack (PA 6), unauthorized access (or inappropriate use of legitimate access by employees) has considerable implications; one can create, modify or erase templates and hence identities. A more extended view of this PA involves the linking of the enrolled template to another person – not the subject of the enrolment, which however surpasses the technological borders and mainly concerns the steps taken initially to verify the identity of the subject whose biometric data will be captured in the system. Hence, if either the enrolled biometric or the personal data provided belong to another person, then their linking and its consequent use by the applicant comprise a serious security breach. Also, it is possible

[1] http://www.ccc.de/biometrie/fingerabdruck_kopieren?language=en

to intercept the transmission from the template to the matcher and force a false positive or false negative (PA 7), or attack the decision-end point (PA 8) of the system which is binary (Yes for authorizing access and No for restricting it). In the latter scenario, if the decision-end of the system is compromised (PA 8) then the biometric data supplied to the device becomes irrelevant. The attacker can choose to either invariably restrict or grant access to anyone, or change right of access as desired.

There are various indicators that point towards biometric system performance; by using the word ‘system’ we denote all the processes as outlined above to the point where the end-user receives clearance for accessing a service and is successfully (or not) authenticated. Hence, we do not strictly mean the device itself. The first indicator results from failure adequately to register with a biometric device and is described as the *Failure to Enrol Rate* (FER). This occurs when a person’s biometric is either unrecognizable, or when it is not of a sufficiently high standard for the machine to make a judgment, something that does not allow the user to enrol in the system in the first place. The second indicator is the *False Non-Match Rate* (FNMR)[2] that occurs when a subsequent reading does not properly match the enrolled biometric relating to that individual, something that results in *Denial of Access* to services. The third indicator is the *False Acceptance Rate* (FAR) and is considered to be the most crucial security error of a biometric system; it is the measure of likelihood that an incorrect identification or verification takes place with a person being accidentally identified as someone else and subsequently gaining access to the services of the rightful biometric holder. It is important here to note that the last two indicators (the FNMR and the FAR) are mutually exclusive. This means that trying to increase the *FAR* in order make it harder for impostors to enter the system then authorized individuals will face difficulties in accessing it and thus the *FNMR* will also increase. However, as security includes not only blocking unauthorized people from accessing the system but also allowing authorized individuals to enter the system, the impact of these rates to the performance and the effectiveness of a biometric system is significant. Hence a trade-off between these two rates is required and this is determined mainly by the application field of the biometric

[2] Also known as False Rejection Rate (FRR)

system. An example of this trade-off can be found in the POLYMNIA system, an intelligent cross-media platform for the production of custom video souvenirs for visitors to leisure and cultural heritage venues, developed in the context of the FP6 IST POLYMNIA project[3]. This application has a strong requirement for a low FNMR ,stemming from the need to include the whole tour of the visitor around the venue, resulting in a higher FAR, which is translated into a higher possibility of including some shots of other visitors in the venue in the video souvenir. Although the latter is not preferable, it does not comprise a system requirement of high importance, as it might in the case of security-oriented application.

Beyond some of the more strictly technical aspects of biometric security such as those discussed above, we acknowledge the existence of a multitude of other factors that are central to IS security regardless of the technological implementation. No matter how much improvement we see in the technology itself, other factors will continue to influence IS security and these will constitute the core of a socio-technical approach to security. In this sense, biometric technologies are no different to any other technology. The security of infrastructures that incorporate biometrics is therefore greatly influenced by social and economic factors, as well as their interplay. Technology *per se* remains important, but the context within which technology operates gives rise to myriad security vulnerabilities.

Such a shift in emphasis is also clearly reflected in the security domain. Despite the fact that governments and organizations have been taking additional steps to ensure the security of their data in recent years, nevertheless security breaches have increased. In a world that is becoming more and more dependent on technology, the label of “insecure” can be disastrous for an organization (Solms 1998). In the UK alone, computer crime has cost £2.4billion over the past year where according to the 2005 review of the National Hi-Tech Crime Unit, a staggering 90% of the companies suffered a computerized break-in, and only 1% of that did not result in data theft (Knight 2005). This constitutes a 6% increase from the year before while the study recognizes that the attacks have become

[3] FP7 POLYMNIA project, http://www.polymnia-eu.org

more elaborate and there is a growing professionalism in the cases examined (ibid). At the same time, it is found that such a growing professionalism takes more and more advantage of ‘social engineering’ methods in order to attack the security of various systems (Marks 2005).

The comments above illustrate the security context that biometrics will be used to address. With biometric technologies and the previous comments in mind, there is an additional security concern that has to be addressed. Irrespective of the effectiveness of the technology *per se*, social engineering methods to undermine the security of biometric implementations will have to be stressed and their implications will have to be factored in, as well as prudently managed. If it is possible to bribe an employee that has access to the biometric data (and/or the templates) then there is no point bothering with the technical aspects of bypassing security. Corruption, always present in one form or another, will find its way to undermine biometrics security. It is therefore crucial that principles of information management pertaining to biometric implementations are explicitly adopted for this purpose and that processes are put in place to ensure effective management and event-handling of cases where security breaches occur. Adopting international standards such as ISO17799 (now revised as 27001) that deal with the security of information systems becomes a necessity (Solms 1999) owing to the nature of sensitive biometrics data, hence both government agencies and businesses should be seeking certifications against relevant international security standards. Top management support, understanding the risks and assets of information, educating on security, dissemination of a clear security policy to the employees, as well as reviews and evaluation on performance are crucial elements amongst the several success aspects of security standards (Li, Hing et al. 2000).

While this section on biometric security has focused mostly on security concerns, that does not mean that biometrics have limited potential for enhancing security; quite the contrary. Biometrics promise enhanced security for authentication and verification and a testament to such a promise is the increased interest from both governments and businesses who seek to adopt biometric systems for their purposes. Information Systems security however is much broader (with technical security being just a subset) and we seek to stress that additional research needs to be done for biometric implementations and those aspects of security that cannot be reduced to just bits and bytes. Providing a secure computing base is one thing; establishing a secure environment and consideration for the business processes is quite another (Solms 1996; Solms 1999)

Security and Privacy

Biometric technologies are claimed to enhance security in a variety of application fields (Walters 2001). One aspect of such a security enhancement is the protection of personal data by limiting and monitoring access to data such as ethnicity, race, religion and health that are considered sensitive and could be jeopardised. Unauthorized individuals are not allowed to access database records that contain this biometric data, while the transaction history in the biometric system provides information on the persons who have accessed the transaction records, along with the temporal information of their actions. Taking into account that biometrics aim at combating the security vulnerabilities of the conventional identification and authentication methods, biometrics are regarded as *privacy guards*. Conventional identification and authentication relies mostly on unique identifiers such as PINs, passwords and smart cards that can be fraudulently stolen but easily replaced; the major difference with biometrics is that they are truly unique (issues of identical twins are still under research) and irreplaceable, even though they too can sometimes be easily jeopardised and used.

Biometric encryption is a technology resulting from the merging of biometrics with cryptography. It is used to complement existing cipher systems in key management with the biometric data being part of the process of establishing the private encryption key or the electronic signature. Encryption is a mathematical process that transforms data from their initial form to an unintelligible form using a coding key. Hence in the case of biometric encryption, biometric data are used in order to encrypt or decrypt data. Taking into account the rapid increase of information exchange via the Internet, as well as the increased need for protection of sensitive data stored in databases connected to open networks, biometric encryption aims at protecting this information and hence act as a privacy enhancing technology (Tomko 1998).

Although biometrics seem to be an integral part of many applications that – some would argue – improve everyday life, increase security and serve as privacy enhancing technologies, they also constitute a serious threat to the individual's privacy. Just as an affirmation might be simultaneously be both true and false (Pinter 2005), so can biometrics simultaneously act *for* and *against* privacy. The interrelatedness of security and privacy is hence once more highlighted in this way, as security becomes the balancing force that determines whether biometrics are *for* or *against* privacy. The mere act of using biometric technologies to capture sensitive biometric data constitutes an immense privacy concern if security is jeopardised, whereas in a scenario where security remains intact, privacy is enhanced and identity theft becomes significantly more difficult. However, as experience shows, there is no such thing as perfect security and hence biometric implementations are likely to see trade-offs between the two ends of the privacy spectrum (truly enhanced or several jeopardised). This makes vital the need for prudent management of the cases where security is threatened. *These threats which are embodied in biometrics and source from both the vulnerabilities and capabilities of biometric systems* are described in the following paragraphs.

Privacy concerns

As already described in the previous section, existing biometric systems include potential security risks which in turn might lead to potential privacy risks. These privacy risks are heightened by the technological vulnerabilities of biometric systems – no biometric system offers 100% success in correctly identifying or verifying individuals registered to the system. Furthermore, an attempt to increase the number of true positives actually contributes to an increase in the false positives as well! As this results in high costs for the organizations using these systems and client disruption, a high integrity universal biometric system could be a rather ideal solution, which in turn however carries high risks with respect to privacy and autonomy (Davies 1998).

The Electronic Privacy Information Centre (EPIC)[4] identifies 4 main concepts of privacy[5]: (1) bodily privacy, (2) territorial privacy, (3) information privacy and (4) *informational privacy*. Bodily privacy refers to the protection of physical selves against invasive procedures, while territorial privacy sets limits on intrusion into domestic and other environments. Information privacy involves rules for the handling of personal data and the privacy of communications in the form of mail, telephone and other forms of communication exchange. *Informational privacy* which incorporates a more descriptive definition and constitutes the main privacy aspect biometric technologies deal with, comprises the establishment of rules governing the collection and handling of personal data such as credit information, medical and government records (also known as "data protection") with any secondary uses of that information constituting violation of the person's right to control it (Banisar 2000).

As already stated, biometric data are highly personal data with the greatest power and privacy threat deriving from their tight link with their owner's identity. The gradually increasing use of biometrics in various fields and the vision of their application as unique identifiers in large-scale – or even universal – applications might deter amateur thieves.[6] However, this perceived increased value of biometric data as unique identifiers offering access to a variety of applications in numerous fields offers a more worthwhile challenge to determined "professionals" to obtain possession of this data, in order to access, modify or bypass it.

Following the security analysis presented in Figure 1, the attempts of a potential impostor with no IT expertise or access to the template databases will only focus on PA1 through the provision of fake or stolen biometric data, a key identity fraud case. In existing

[4] http://www.epic.org/

[5] http://www.apiicc.org/apiicc/Lecture/IT_HRD/10.pdf

[6] Comments of the Electronic Privacy Information Center to the Federal Trade Commission

conventional identification or verification systems, such as credit card-based or password-based systems, vulnerability to attacks that mainly focus on *identity fraud* constitutes one of the major privacy concerns (USTreasury 2005). The latter refers to stealing and using identifiers, seeking mainly at capturing the individual’s privileges in order to get special permits, hiding a personal identity or committing financial fraud, money laundering, computer crimes, alien smuggling or even terrorist actions.

Implementing authentication or identification systems based partially or fully on biometrics, or integrating biometrics in existing systems, aims to benefit from the potential of biometrics, a potential based on their uniqueness for any person and the difficulty of being easily and accurately reproduced. However, both bodily and informational privacy are at stake. The first is threatened in PA1 by forcing the person to enter his/her biometric data into the system or even by removing it (e.g., cutting a finger), mainly performed by rather “amateur” criminals, who attempt to attack the biometric system by collecting the biometric information directly from its owner. The main points of attack that comprise intrusion of the individual’s information privacy are PA1 and PA6, through collecting or even faking the person’s biometric traces. In an attempt to compare the impact of these two points of attack on the informational privacy, an attack on the template (PA6) of a person’s biometric data –insertion, modification or deletion – is regarded as a much more serious threat, since it allows for a series of incidences of false positives before being actually detected. This threat actually increases by the fact that biometrics are permanent identifiers, in contrast with a password or a smart card, whereas the options for alternatives are limited (two eyes, ten hand fingers). *Biometrics spoofing* is therefore both a peril and a challenge that biometric systems should confront, especially since biometrics are generally exposed publicly (facial images are easily captured, fingerprints can be collected from any place the person touches). Technological solutions of many of these issues are known as *anti-spoofing techniques*.

The main principles supporting data protection include data minimization, lawful processing, data subject control, disclosure limitation and purpose specification[7]. An

[7] http://www.apiicc.org/apiicc/Lecture/IT_HRD/10.pdf

intense concern surrounding the governmental and commercial applications of biometric technologies is the systematic *collection* and use of biometric data which could result in being *unnecessary and more importantly unauthorized* (Cavoukian, 1999). In the case of non-intrusive biometric technologies especially, the collection of biometric data can take place even without the person being aware that they are targets of the biometric system. By the term ‘non-intrusive biometric technologies’ we signify biometric technologies not easily detected by the subject, mainly due to the fact that such technologies operate without requiring interaction with the person, such as in camera-based face recognition. Taking into account the fact that such technologies are part of smart surveillance systems applied either at public access facilities or private areas (e.g., at the office or stadiums) for security purposes, the fear that an electronic trace of every person’s movements is processed and stored is real, and that the power of authorities will grow and civil liberties will be violated.

As anonymity is regarded as the ability of people to conduct their lives and business without making their activities known to others, then the right of maintaining *anonymity* in daily life seems to be at stake (Woodward 1997; Arndt 2005). Wiretapping that takes advantage of voice recognition technologies and video surveillance is regarded by many as a highly intrusive form of surveillance and an investigative technique that should scarcely be used. Furthermore, what is worrying is that many cameras capturing images from squares, street corners or avenues can be accessed through the Internet. The implementation of biometric passports has raised grave concerns over the protection of travel data as well. In an effort to draw attention to the threats associated with Machine Readable Travel Documents (MRTDs), the researchers in FP6 FIDIS project[8] created the “Budapest Declaration on Machine Readable Travel Documents (MRTDs)” [9] which also included recommendations to governments and industries. Although this concern may not be as worrying as where financial and medical data could be jeopardised, fears have been expressed that travellers are now seen and treated as potential terrorists and thus surveillance targets (PHR 2004). Considering that some of these systems, aiming at

[8] http://www.fidis.net

[9] http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf

higher security through situation awareness (e.g., identification of abnormal behaviour compared to usual behaviour), not only perform identity tracking but also activity identification and tracking (Foresti 2005; Hampapur 2005), and that the number of cameras and other devices is increasing rapidly, the privacy risks seem to be higher than initially expected. Clearly, all the aforementioned side-effects on privacy are different and crucial manifestations of the problem of data re-purposing (data collected for one purpose and used for another).

A serious social threat is the use of biometric surveillance systems in order to monitor the activities of certain groups of people, such as those of a particular ethnicity or convicted criminals. Especially after 9/11, we are witnessing an unprecedented regulatory pressure whereby freedom of information, privacy and online free speech are under continuous scrutiny (Davies 2002). Information which categorizes individuals into these groups could either be the result of information disclosure from companies or governments – encroaching on the disclosure limitation principle of data protection - or of further processing of the captured biometric data and the extraction of *soft biometrics*. This term refers to human characteristics that provide information about an individual but cannot sufficiently differentiate any two individuals (Jain, Dass et al. 2004). These characteristics include a person's gender, ethnicity and eye colour. The applications of biometric systems that embody soft biometrics range from query filtering during identification (by reducing the number of records to be included in the matching process) or verification to statistical applications. Although their use could improve the performance of biometric systems as far as both speed and robustness are concerned, their application domain does not currently focus on authentication and identification; they are used for statistical purposes, such as the assignment of a person to a religious or ethnic group. Fears about the use of such applications revolve around the provision of special privileges to specific groups of people and the denial of services to individuals of other groups resulting in discrimination and racism.

The extraction of soft biometrics can either be made real-time on the captured biometric data or by the results of post-processing of this data. The latter in most cases implies the storage of raw data (e.g., a person's image) instead of just the templates, a choice that is justified by the effort to create flexible systems that do not require data re-collection from enrolled individuals when changes to the system are required. As raw data can be information-rich and provide additional information on a person such as health status, ethnicity or gender, attacking a database with stored data of this type (PA6) would result in a greater privacy threat than an attack on a database containing encrypted biometric templates. Hence, after the creation of the reference template, the original biometric or raw data should not be retained (Cavoukian 1999).

As biometric data are highly personal, they could be used as universal human identifiers linking together data about a person concerning their daily life, financial transactions, trips, and other sensitive data - such as ethnicity, religious beliefs, medical record, race, criminal record – and thus composing a near-complete description of a person and his/her activities. Amounting to a combination of encroachment of disclosure limitation, data subject control and purpose specification principles of data protection, such information linkage constitutes a great privacy concern. Therefore, although data linking could lead to a better provision of services by proposing products that best fit a person's preferences, it also constitutes a threat to the person's privacy, as a *profile* for each person could be systematically created and used without their consent. For example, what if insurance companies could link their customers' records with their medical records? Persons' data linking or data collection and use without their consent could be regarded as part of the overall issue of *unauthorized information use* (ibid). When consumers consent to the use of a unique biometric trait to make a transaction through an ATM or access a computer centre, they assume that their biometric data will be used for that particular purpose and only. Especially in the private sector that most decisions are made based on the economic gain, there is the overarching concern that companies will try to exploit fully the capabilities of biometric technologies and disregard the privacy cost. An example is the extraction of medical information from the collected biometrics – especially DNA, fingerprints and iris - and its use against the individual's interest, such as for discrimination purposes.

The potential for profiling and identity fraud has contrasted the otherwise innate reluctance and cautiousness of the financial sector in the introduction of biometric technologies, mainly due to its high security requirements and concerns about negative customer reaction (USTreasury 2005). Privacy risks in financial data are posed, such as account balances, credit card data, tax refund data, transaction history and many others including mainly the exposure of this sensitive information to unauthorized people and its fraudulent manipulation (Potter 2002). Moreover, the establishment of the initial relationship of the customer with the financial institution is a sensitive issue, since at this point the institution does not have an enrolled template to match the data provided by the applicant. Hence if either the enrolled biometric or the personal data provided belong to another person (PA6), then their linking and its consequent use by the applicant could lead to a series of identity fraud actions.

Conclusions

This review of the most crucial security and privacy aspects pertaining to biometric implementations shows that there are serious concerns and that more research needs to focus on aspects that go beyond the purely technical domain (i.e. especially related to Information Systems Security), and recognises that biometrics is only part of the solution – but also part of the problem. In cases where applications of high security standards and requirements are required, supervised enrolment by trained and trusted staff may ensure the quality and the reliability of the data enrolled. Similarly, monitoring the use of the system can in many cases be supervised by staff in order to avoid spoof attacks and the unintended provision of false biometric features by the person to be authenticated or identified. Nevertheless, efforts throughout past years to reduce and eventually eliminate these threats have been carried out by designing and implementing new technologies. There is research into anti-spoofing techniques aiming at making biometrics authentication and identification systems intelligent in distinguishing between presented real and fake data. Special techniques that are applied at the time and place the person tries to gain access to the biometric system are developed performing "liveliness checks" and thus trying to detect cases of biometrics provided from artificial equipment.

Advanced techniques of data encryption, database security and network security are also amongst the suggested technological solutions for privacy invasion attempts, whereas many overlook the fact that privacy should be an integral part in the design and the implementation of systems including biometrics technologies.

It has to be recognized however that technology itself is not a panacea. The real-life challenges in security and privacy are extended into the social, political and economic sphere and triggered by the technological artefacts themselves. There are no cause-and-effect relations amongst technological implementations and the resulting infrastructures, as a variety of contextual elements influences the implementations themselves. Therefore, more research concerning biometric implementations is needed to incorporate aspects of biometric security and privacy that go beyond the purely technical domain with its rational-logical solutions. Issues such as data protection, new opportunities for criminality and the handling of false positives and false negatives should be treated under a new perspective of a broader Information Systems Security; a perspective that will recognize both the validity of such an approach and of advancing biometric security and privacy beyond the scope of strictly technical solutions.

Bibliography

Arndt, C. (2005). The loss of privacy and identity. Biometric Technology Today.

Banisar, D. (2000). Privacy and Human Rights: An International survey on privacy laws and developments. Washington, Electronic Privacy Information Centre.

Cavoukian, A. (1999). "Consumer Biometric Applications: A Discussion Paper." from http://www.ipc.on.ca.

Davies, S. (1998). "Biometrics - A Civil Liberties and Privacy Perspective." Information Security Technical Report **3**(1): 90-94.

Davies, S. (2002). "A Year After 9/11: Where are we now?" Communications of the ACM **45**(9).

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM **43**(7).

FIDIS (2005). D3.2: A study on PKI and Biometrics. M. Gasson, M. Meints and K. Warwick**:** 1-138.

Foresti, G. (2005). Active Video-Based Surveillance System. IEEE Signal Processing Magazine**:** 25-37.

Hampapur, A. (2005). Smart Video Surveillance. IEEE Signal Processing Magazine**:** 38-50.

Jain, A., S. C. Dass, et al. (2004). Can soft biometric traits assist user recognition? Proceedings of SPIE, Biometric Technology for Human Identification, Orlando, Florida.

Knight, W. (2005). "Computer Crime boom costs UK millions." New Scientist, from http://www.newscientist.com/article.ns?id=dn7233.

Li, H., G. Hing, et al. (2000). BS7799: A Suitable Model for Information Security Management. AMCIS, Long Beach, California.

LSE. (2005). "The Identity Project." from http://is.lse.ac.uk/IDcard/.

Marks, P. (2005). "Attempted cyber-heist raises keylogging fears." from http://www.newscientist.com/article.ns?id=dn7168.

Matsumoto, T., H. Matsumoto, et al. (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems. Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE.

PHR. (2004). "Threats to Privacy." from www.privacyinternational.org/threats2004.

Pinter, H. (2005). "Art, Truth and Politics." from http://nobelprize.org/literature/laureates/2005/pinter-lecture.html.

Potter, E. J. (2002). "Customer Authentication: The Evolution of Signature Verification in Financial Institutions." Journal of Economic Crime Management **1**(1).

Solms, R. v. (1996). "Information Security Management: The Second Generation." Computers & Security **15**: 281-288.

Solms, R. v. (1998). "Information security management(1): why information security is so important." Information Management & Computer Security **6**(4): 174-177.

Solms, R. v. (1999). "Information security management: why standards are important." Information Management & Computer Security **7**(1): 50-57.

Tomko, G. (1998). Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy? Privacy Laws & Business, 9th Privacy Commissioners/Data Protection Authorities Workshop, Spain.

Uludag, U. and A. K. Jain (2004). Attacks on biometric systems: a case study in fingerprints. Proc. SPIE-EI 2004, San Jose, CA.

USTreasury. (2005). "The use of technology to combat Identity Theft - Report on the study conducted pursuant to section 157 of the Fair and Accurate Credit Transactions Act of 2003." from http://www.treas.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf.

Walters, G. (2001). Human Rights in an Information Age: A Philosophical Analysis. Privacy and Security: An ethical analysis, University of Toronto Press.

Woodward, J. (1997). "Biometrics: Privacy's Foe or Privacy's Friend?" Proceedings of the IEEE **85**(9).