Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 424–431
© MIR Labs, www.mirlabs.net/jias/index.html

# Identification Using Biometric Technology: Issues and Attitudes

**Shamim Khan[1] and Pinar Gurkas[2]**

[1]Columbus State University, School of Computer Science,
4225 University Avenue, Columbus, GA 31907, USA
*s.khan@computer.org*

[2]Department of Psychology, Clayton State University,
2000 Clayton State Boulevard · Morrow, GA 30260, USA
*pinargurkas@clayton.edu*

*Abstract:* **The process of establishing identity is performed routinely for preventing unauthorized access and for aiding criminal justice. Biometric technology, which involves the use of some unique physiological and behavioral characteristics, is being increasingly used for this purpose. Due to its intrinsic nature, authentication based on biometric technology is much less susceptible to compromise than traditional methods such as passwords. But the personal nature of biometrics and the ease of replicating and sharing it in digitized form naturally raise questions about its usability, security and privacy aspects. This paper examines issues of concern relevant to the use of this relatively new technology. It reports on an investigation into people's attitude towards the use of biometric technology. It is based on a survey of the most common biometrics: facial image, fingerprint, voice, hand geometry, keystroke dynamics, iris scan, retina scan, and signature analysis. Three domains regarding attitudes are studied - how comfortable survey participants felt with biometric technologies, how secure they thought these technologies were, and how intrusive they thought these technologies would be if used on a daily basis. Possible differences in attitude towards this technology based on gender, age, personality and ethnicity are analyzed.**

***Keywords***: Identification, biometrics, biometric technology, user perception.

## I. Introduction

The word biometric(s) stems from the Greek words 'bio' meaning life and 'metric' meaning to measure. As a noun, it refers to physiological characteristics – for example, someone's fingerprint. As an adjective, biometric relates to anything dealing with the use of such characteristics – the most well-known example of this being biometric technology (also referred to simply as biometrics).

Biometrics has existed throughout history as a tool for identifying people; the use of some distinctive feature such as a unique scar, or more recently, the use of fingerprints are examples of this. Although traditional use of biometrics such as fingerprints has been mainly for the purpose of criminal investigation, the proliferation of information systems that store massive amounts of data related to all aspects of people's lives, has provided impetus for the use of biometrics to protect confidentiality of information by preventing unauthorized access. Fighting crime using biometrics has also taken on a new dimension with the recent increase in the threat of terrorism, where the ability to accurately and efficiently distinguish between the innocent and the suspect can lead to a significant saving of resources, and potentially, lives.

A very important task in information assurance is user authentication ("Am I who I claim to be?") before allowing access to information. A more challenging task is that of recognition ("Who am I?"), often used in fighting crime and countering threats to public security. Traditionally, knowledge-based (something a person knows) and token-based (something a person possesses) approaches have been used for personal identification [1].

The most well-established method for user authentication is knowledge-based and it relies on the use of passwords. Although relatively simple and inexpensive to implement, passwords can be forgotten, shared, or stolen. Their use for authentication is becoming increasingly insecure due to the sheer number of passwords one has to remember these days. According to one survey of enterprise end-users reported in [2], nearly half of the respondents said they keep their passwords saved in plain text on their PC or on a handheld device. Writing down passwords on a piece of paper or around personal computers was also reported. While such practices lead to increased risks of security breaches, strict enforcement of secure password management policies such as frequently updated strong passwords often lead to IT support staff having to routinely reset passwords and unlock computers. Lost productivity due to password problems and the waste of IT resources in helping affected users add to business costs. The alternative token-based approach to user authentication also has its deficiencies. Tokens, such as smart cards and magnetic stripe cards can be lost, stolen, duplicated, or left at home. The major drawback of both knowledge and token-based identification systems is that they recognize an impostor in possession of the relevant knowledge or token [1].

With the increasing use of information technology and automation in all aspects of life, the need for efficient and reliable identification is greater than ever. Biometrics in the information technology field is a relatively new concept of identifying information system users and protecting such systems from intruders. Given the obvious deficiencies of traditional user authentication techniques, biometric technology has become an active area of research and development. Only biometric authentication is based on intrinsic personal features that have two very important advantages over traditional methods. Except in extreme situations (for example, due to accident or disease) they cannot be lost. Secondly, unlike a password or smart card, they cannot be shared. This makes biometric-based identification much less susceptible to compromise. Given its advantages, biometric technology is expected to be increasingly used in applications for improving security in physical installations such as airports, as well as preventing identity theft in financial and social services.

While biometric technology has been making significant progress in the last two decades or so, its application is yet to become widespread. There are a number of factors behind the relatively slow spread of this technology – some are technical such as reliable acquisition and levels of accuracy and consistency, while others have to do with issues like user-acceptance and ethics. This paper introduces current biometric technology and related technological as well as non-technological issues. It next gives a brief account of some research done on user perception of this technology before presenting the initial findings of a study to investigate possible links between user perception and user background characterized by gender, age, ethnicity and personality traits.

## II. BIOMETRIC CATEGORIES

Biometric information can be categorized into two broad groups - physical and behavioral.

### *A. Physical Biometrics*

Physical biometrics pertains to any form of biometric that is found on and measured off the human body. Common physical biometrics include fingerprints, iris and retinal scans, hand geometry, facial image, and DNA pattern. A key component of physical biometrics is that they hardly change over time. A person’s fingerprint, eye, and DNA are unlikely to change through their lifetimes except in highly unusual circumstances. Facial recognition is the exception to this property of invariability. People’s faces can change with age, use of glasses to help vision impairment, or changes in hair style or facial hair.

### *B. Behavioral Biometrics*

Behavioral biometrics encompass the habitual information of a person. It can be captured and analyzed through the use of signature recognition, keystroke analysis, and voice analysis. Although each person’s voice is unique in pitch, voice analysis focuses on the way a person speaks. Unlike physical biometrics that remain relatively constant over time, behavioral biometrics can change in a very short period of time. For example, people might not have a consistent style signature. On the other hand, behavioral biometrics are relatively inexpensive, less intrusive, and can be changed if compromised [3].

## III. OPERATION OF A BIOMETRIC SYSTEM

Regardless of the type of biometrics, in order to establish identity, there must be a way for a biometric system to collect, store, and compare the biometric data captured from its users. Two main processes, called enrollment and verification, accomplish this goal.

### *A. Enrollment Process*

Enrollment and verification involves the capturing, transformation, transfer, and storage of biometric data to acknowledge who the person claims to be [4]. The enrollment process is where a user inputs their data into a biometric system for matching with future inputs. The first step in the enrollment process is to capture a user’s raw biometric data through a biometric capture device like a camera, microphone, or fingerprint reader. Once the data is collected, a template for that user is made. Normally this template is a composition of multiple data captures, which helps create a more generic template for that user. This ‘reference template’ is then transmitted and stored in a database [4].

### *B. Verification Process*

As shown in figure 1 below, the first step in the verification process is similar to the enrollment process. The user’s raw data is captured and made into a ‘sample template’. This sample template is used to verify the user’s identity. There are two main methods of comparing a user’s sample and reference templates. Recognition takes the sample template and compares it against all other templates in the database. Verification compares the sample template against the reference template of who the unknown user claims to be.

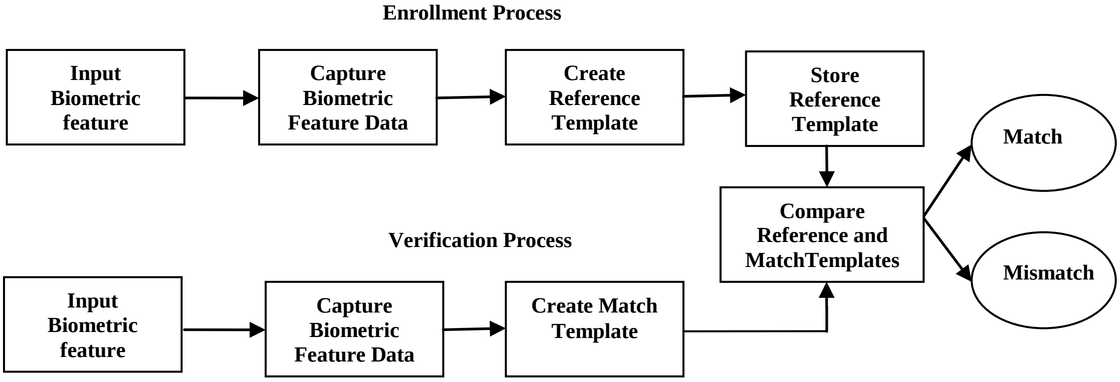

**Figure 1**. The operation a of biometric identification system.

# IV. BIOMETRIC TECHNOLOGY ISSUES

Apart from possible practical difficulties associated with the acquisition, storage and processing of biometric data in an efficient and secure manner, a number of non-technological issues are also of concern when it comes to the adoption of this rapidly maturing technology. These issues are determinants of user acceptance from the viewpoints of legality, ethics, society, culture and personal privacy. A number of such technological as well as non-technological issues are discussed below.

## *A. Selection and use of biometrics*

Ideally, for any biometric feature to be selected as a basis for verification or recognition, it is expected to exhibit the following properties:

- Universality: Every person should possess the characteristic.
- Uniqueness: No two people should share the same value for the characteristic.
- Permanence: The characteristic should not vary with time.
- Collectability: It must not be too difficult to collect and measure the characteristic.
- Performance: The method must deliver accurate results under varied environmental circumstances.
- Acceptability: The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.
- Circumvention: The technology should be difficult to deceive.

There are three common terms used to assess the quality of a biometric system's enrollment and verification process. These measures are the FTE (Failure to Enroll) rate, which shows how well the system is able to acquire and enroll users into the system, the FAR (False Acceptance Rate), which is how often the system grants access to intruders, and the FRR (False Rejection Rate), which is how often the system denies access to legitimate users [5]. A sample template and the corresponding reference template (if any) are unlikely to be exact matches. Because of this, a threshold value is used to determine how close the sample template is to the reference template [4]. The threshold can be manipulated to adjust the FAR and FRR rates. A reduction in the FAR value usually results in an increase in FRR. Consequently, the right balance between these two conflicting system characteristics has to be reached so that a biometric system's reliability needs are met. In addition to adequately low FAR and FRR rates, an acceptable FTE rate is also essential for the type of biometric chosen for a system. As an evolving technology, biometric systems need to increase both accuracy and speed when it comes to the enrollment and verification processes.

## *B. Legal and Ethical Issues*

The use of biometrics is not entirely new. Fingerprints and facial images have been routinely used long before computers became commonplace. But the use of information technology and new types of biometrics has given rise to the need for standards among biometric systems [6]. Work on standards in the use of biometric technology is currently in progress at international and national levels [7], [8]. Ideally biometric data should be classified as personal data, and fall under appropriate legal protection; for example, biometric data should be gathered only with user consent [9]. There are currently no set guidelines on what a system's FTE, FAR, FRR and threshold need to be, or what information is allowed to be collected and stored. There is also no standard way to collect and store biometric data. All these factors can make it difficult for biometric evidence to be admissible in court [6]. There is also the issue of providing access to a biometric system for users with a documented disability. Depending on how the law is interpreted, designers may be forced to consider alternative methods of granting access to people who are unable to enroll in the biometric system.

Legal and ethical issues are often closely tied together, and biometric technology is no exception. A difficult ethical issue relevant to biometrics is social exclusion. It can affect biometrics in that not everyone may be able to enroll into a biometric system and gain the benefits of the latest technology. A study found that about 0.62% of one of the survey's subgroups was unable to enroll in a biometric system [6]. People with a physical and/or learning disability along with the elderly can have difficulty enrolling in a biometric system (in terms of accuracy and time spent enrolling). This can lead to certain groups of people being excluded from everyday activities that should be available to everyone.

## *C. Socio-cultural and Privacy Issues*

Issues with the use of biometric technology can also arise due to one's religious and cultural background, and prevailing social and political situation [10]. One possible obstacle to biometric acceptance may be stigmatization. Some communities associate fingerprinting with law enforcement and acts of criminal behavior [9]. Subjecting oneself to procedures involving physical exposure and/or contact may become an issue with specific religious groups. Along with possible stigmatization is the fear of tracking; the ability to monitor in real time an individual's actions or to search databases that contain information about these actions [9]. Individuals might have a fear of "Big Brother" watching them, and collecting information about their actions without their knowledge.

There is also the concern that biometric data will be used to stereotype or classify people. A study conducted in Sweden found a link between data collected from iris scans and different personality types in adulthood [9]. This can lead to the fear that employers who ask for biometric data during the hiring process might discriminate between potential hires based on biometric data.

Another popular concern from the security and trust standpoint is that of function creep. When applied to the field of biometrics, function creep refers to the issue of biometric data being used outside of their original purpose [6], [11], [9]. Organizations selling or passing on personal information such as names and addresses to others without seeking consent is an ongoing phenomenon. But the unique and permanent nature of biometric information adds a more serious dimension to such a breach of confidentiality. The damage caused by a stolen password or token can be minimized by replacing it with a new one. But biometric features such as fingerprints or retinal patterns cannot be changed if identity theft is suspected.

According to the International Biometric Group [12], it is the nature of deployment, rather than the type of biometric being used, that determines how this technology can affect privacy. The factors determining the nature of deployment and hence the degree of invasiveness are outlined below.

- Overt vs. Covert: Deployments in which users are aware that biometric data is being collected and used are less susceptible to privacy violations.
- Opt-in vs. mandatory: Mandatory biometric data collection is more likely to be viewed with suspicion.
- Authentication vs. recognition: Biometric database searches for finding matches for recognition purposes is more susceptible to privacy-related abuse than a 1:1 matching for verifying identity.
- Fixed duration vs. indefinite duration: The use of biometrics for a fixed duration is less likely to have a negative impact on privacy than one used indefinitely. Longer deployment increases the likelihood of function creep.
- Public vs. private sector: While government collection of biometric data without proper controls can be problematic, abuse by private sector companies for marketing or profiling is more likely.
- Role of the individual: Expectations of privacy are dependent on the capacity in which a person is interacting with another person or institution, such as - anonymous individual, customer, student, traveler, citizen, employee, prisoner.
- Ownership of biometric data: User ownership involving control over collection, usage, and disposal of biometric information is more likely to be privacy-sympathetic than public or private institutional ownership.
- Personal vs. centralized storage: A central database for biometric data is more vulnerable to misuse than one in which biometric information is stored on a user's PC or on a smart card.
- Behavioral vs. physiological biometric: Behavioral biometrics such as voice recognition and signature-scan are less likely to be a security concern compared with physiological biometrics like finger prints and retinal scans, which cannot be changed by the owner.
- Templates vs. identifiable data: Some organizations retain and use both identifiable data, such as images, and biometric templates at the same time. Identifiable data are more sensitive than biometric templates, and are more likely to lead to privacy-invasive usage.

## V. CURRENT RESEARCH ON USER ATTITUDES

Issues such as those mentioned above may stem from how the users interact with a biometric device, and how they perceive the risks and benefits of using biometrics for identification over traditional knowledge and token based systems. There have been a number of reported studies that gathered data about user acceptability and usability of biometric technology [13] [10], [14]-[17], [6]. All these surveys, except one, were solely questionnaire-based. The study reported in [6] used a mock biometric system that participants were asked to use before responding to a survey. This approach, although attempting to gather feedback on actual user experience, was restricted to the experience of only one type of biometric.

All these reported survey methods yielded results that showed that participants have heard of biometrics, yet were skeptical about using the technology [14], [11]. In most of the surveys, a relatively low percentage of participants had used a biometric device. The oldest of these surveys, reported in a journal article published in 2004, found that only 6% of its participants had used a biometric device [16] . This serves as an indicator that at least until the early 2000s, biometrics had not had a prominent presence in people's everyday lives. This is in contrast with the findings we reported below in section 5.

Although the reported surveys provide a wealth of information, most are limited in some way or other such as - surveying only Computer Information Systems (CIS) students [17], surveying a large college class of mostly Caucasian students aged 18 – 21[11], having a small participation pool (under 50 participants) [14], and the age of most participants surveyed being under 30 years [13], [11], [17]. Surveys that included older age groups showed different results in acceptability and usability [16], [6]. This includes the general tendency to avoid biometric systems in favor of a traditional system, and a more difficult time enrolling in a biometric system. Most of these surveys did not consider the ethnic background of their participants. Also, none of these surveys attempted to relate personality traits with people's perception.

## VI. A SURVEY ON USER ATTITUDE TOWARDS BIOMETRICS

As part of an ongoing study of people's perception of biometric technology used for identification, we examined attitudes towards 8 common biometrics used for this purpose: facial image, fingerprint, voice, hand geometry, keystroke dynamics, iris scan, retina scan, and signature analysis. We focused on three domains regarding attitudes: 1) how comfortable participants felt with biometric technologies; 2) how secure they thought these technologies were; 3) how intrusive they thought these technologies would be. In addition to investigating how people felt regarding these three aspects of biometric technology, an additional goal was to look for possible links between attitudes towards these three aspects and a participant's own attributes; gender, age, ethnicity and personality traits among them. During 2009, students in several courses across the university were contacted in their classrooms and invited to participate in the survey. Data collection for this study was completed online using a Web-based survey tool.

We developed a 47-item questionnaire to record participants' thoughts regarding biometric technologies.

They were asked to provide demographic information, and information regarding their familiarity with different biometric technologies. To minimize the effect of ignorance on specific types of biometrics, each question was accompanied, where appropriate, by a brief description of the associated technology. In order to measure individual differences in personality, the Big Five Inventory [18] was used. The BFI is a widely used measure of adult personality. Personality is broadly defined as characteristics that we display consistently across situations. According to one of the most commonly accepted theories of personality, there are 5 dimensions of human personality: neuroticism (i.e.., emotional stability), extraversion( i.e., how sociable a person is), agreeableness( i.e., how trusting, helpful, easygoing a person is), conscientiousness (i.e., how disciplined a person is), and openness to new experience.

Participants were 184 students (67 males, 117 females). Average age of participants was 24 years. Fifty-nine percent of our participants were European-American, 30% were African-American, 4 % were Asian-American, 3% were Hispanic, and 4% identified their ethnicity/race as 'other'. About 49% of participants had a background in information technology (study or work related); the rest were from a non-IT background spanning 20 different areas of study such as English and Nursing. A majority of the participants indicated that they had heard of biometrics. Among the biometric technologies, facial recognition, finger print, and voice analysis were the best known; hand geometry analysis was the least known technology. A majority of participants, 63%, indicated that they had used biometric technologies before. Fingerprint and signature analysis were the most commonly used biometric technologies - used by 40% and 31% of the participants respectively.

Participants' perception of the eight types of biometrics investigated with regard to the three aspects of comfort, security and intrusiveness were found to be as follows:

### A. *Comfort level*

Participants appeared to be most comfortable with fingerprint analysis, with 82% putting it in the first place; voice (67%) and hand geometry analysis 62%) came second and third. The feeling of comfort with fingerprinting may be due to familiarity arising from its longstanding and widespread use. This attitude of comfort about fingerprinting also appears to go against the "criminal stigma" concern mentioned earlier.

### B. *Security*

In terms of a feeling of security, once again fingerprinting occupied the first place among respondents (75%); followed by retina scan (66%) as second and iris scan (65%) a close third. Fewer than 9% of the respondents thought it would be easier to steal biometric information than stealing traditional markers of authentication such as passwords. Overall, biometrics was regarded more positively than the two most popular conventional identifications techniques but opinion was divided; 55% thought it should replace ID cards and 57% thought similarly about passwords. Also, the standard deviation on the security aspect was greater (0.19) compared with those of comfort (0.09) and intrusiveness (0.08).

### C. *Intrusiveness*

Some level of concern was noticeable on the intrusive nature of biometrics. Facial imaging concerned participants most (43%) for being intrusive; followed by retina scan (40%) and iris scan (37%). Given the invasive nature particularly of iris scan, it is interesting to note that physical intrusiveness does not appear to be a major concern, even for an apparently invasive method like retina scan (40%), which requires a person to stare into an infrared beam for a number of seconds at a close range. Overall, fewer than half of the participants seemed worried about this aspect of biometric technology.

### D. *Gender differences in attitudes towards biometric technologies*

In order to explore gender differences in attitudes towards biometric technologies, t-tests were performed on the data. As shown in Table 1 below, there were no differences between male and female participants with respect to how comfortable they felt with biometrics technologies [t(182) = -.74, p> .05], how secure they thought these technologies were [t(182) = .44, p> .05], and how intrusive they thought these technologies would be if used on a daily basis [t(182) = .19, p> .05] .

Table 1. Descriptive Statistics for Male and Female Attitudes towards Biometrics

| **Attitude** | **Male (N=67)**<br>**Mean (SD)** | **Female (N=117)**<br>**Mean (SD)** |
|---|---|---|
| **Comfort** | 28.79 (7.75) | 28.03 (5.95) |
| **Security** | 26.57 (5.41) | 26.94 (5.55) |
| **Intrusiveness** | 23.01 (8.29) | 23.22 (6.38) |

### E. *Differences in attitudes as a function of ethnicity*

In order to explore any differences in attitudes towards biometric technologies based on ethnicity, t-tests were performed on our data to compare European-American and African-American participants – the two dominant ethnic groups in our sample. There were no differences between these two groups with respect to how comfortable they felt with biometrics technologies [t(162) = -.37, p> .05], how secure they thought these technologies were [t(162) = -.77, p> .05], and how intrusive they thought these technologies would be, if used on a daily basis [t(162) = -1.81, p> .05]. Table 2 below presents descriptive statistics for participants grouped by ethnicity.

*Table 2*. Descriptive Statistics for Attitudes towards Biometrics as a function of Ethnicity.

| **Attitude** | **African American (N=55)**<br>**Mean (SD)** | **European American (N=109)**<br>**Mean (SD)** |
|---|---|---|
| **Comfort** | 28.49 (6.43) | 28.08 (6.93) |
| **Security** | 27.20 (6.35) | 26.49 (5.22) |
| **Intrusiveness** | 24.75 (7.16) | 22.61 (7.14) |

### *F. Differences in attitudes as a function of age*

In order to explore the links between personality traits and attitudes towards biometric technologies, we used correlations between scores on three scales of attitudes (namely, comfort, security, and intrusiveness) and age of participants. Age was not related to how comfortable participants were with biometrics ($r = .03$, $p>.05$), how secure they thought these technologies were ($r = -.003$, $p>.05$), or how intrusive they thought these technologies were ($r =-0.13$, $p>.05$).

### *G. Differences in attitudes related to personality*

In order to explore the links between personality traits and attitudes towards biometric technologies, we used correlations between scores on three scales of attitudes (namely, comfort, security, and intrusiveness) and scores representing five dimensions of personality (i.e., openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism). Attitudes towards biometrics were found to be not related to personality traits. Individuals who had more positive attitudes towards biometrics had higher scores regarding how secure they thought these technologies were, and lower scores regarding how intrusive they thought these technologies were (see Table 3 below for details).

Table 3. Correlations between Personality Traits and Attitudes towards Biometrics

| | **Comfort** | **Security** | **Intrusiveness** |
|---|---|---|---|
| **Security** | .58** | | |
| **Intrusiveness** | -.14* | .003 | |
| **Extraversion** | .08 | -.11 | .13 |
| **Agreeableness** | .10 | .10 | -.02 |
| **Conscientiousness** | .04 | .11 | -.06 |
| **Neuroticism** | -.10 | -.13 | -.06 |
| **Openness** | .02 | -.10 | -.03 |

* $p \leq .05$, ** $p \leq .001$, N= 184

### *H. Analysis using clusters*

In order to further explore the nature of the relationship between attitudes towards biometrics and personality traits, a hierarchical cluster analysis was performed on the survey data. We used the squared Euclidean distance as our measure of distance in this analysis. The 3 measures used regarding the perception of biometrics were: comfort with biometrics, security of biometrics and intrusiveness of biometrics. Our five dimensions of personality were: extraversion, agreeableness, conscientiousness, neuroticism, and openness. Participants were divided into 4 clusters. One-way ANOVA was used to determine differences between clusters regarding biometrics and personality traits. Table 4 below provides a summary of the results of the cluster analyses.

The first cluster had 64 participants. These participants overall were not highly extraverted or highly neurotic. They were more agreeable than most others in our sample. Regarding biometrics, there were significant differences between the first cluster and second and fourth clusters. Specifically, these participants were more comfortable with biometrics than those in the second cluster and less comfortable than those in the fourth cluster. The first cluster of participants also believed that biometric technologies were more secure than did the second cluster of participants, and less secure than did the fourth cluster of participants. Hence, the first cluster was composed of those who were not extremely eager to try new things such as biometric technologies; they were comfortable with these technologies and were not extremely concerned about security issues. Among all the participants they found biometrics to be the least intrusive.

The second cluster had 40 participants. These participants were highly extraverted. They were less agreeable and more neurotic than the first and fourth clusters and less neurotic than the third cluster of participants. These participants were the least comfortable with biometric technologies. Intrusiveness was not their major concern as it was for the first cluster. Their main concern was security of these technologies. Among all the participants they found biometrics to be the least secure.

The third cluster had 61 participants. Among all participants, these participants were those who were the least extraverted and most neurotic cluster. They were also less agreeable and less conscientious than the first and fourth clusters of participants. Regarding biometrics there were significant differences between this cluster of participants and those in the second and fourth clusters. Specifically they were more comfortable with biometrics and they believed that these technologies were more secure than did the second cluster of participants. The third cluster of participants had less positive attitudes towards biometrics and they believed these technologies to be less intrusive than did the fourth cluster of participants. Overall, despite the fact that the third cluster of participants included those who were the most timid and anxious in our sample, they did not have extreme concerns regarding security or intrusiveness of biometric technologies.

The fourth cluster had 18 participants. These participants were more extraverted than the first and third cluster of participants. They were more agreeable than the second and third clusters. They were more conscientious than the third cluster of participants. They were less neurotic than both second and third clusters of participants. Among all the participants these participants were the most comfortable with biometric technologies. They did not have extreme concerns regarding security but among all the participants they found biometrics to be the most intrusive.

Based on the results described above, in linking personality with attitudes towards biometrics, three dimensions of personality - extraversion, agreeableness, and neuroticism - should be investigated more extensively in the future.

Table 4
Cluster Analysis by Attitude to Biometrics

| **Attitude Metrics:** | **Comfort** | **Security** | **Intrusiveness** |
|---|---|---|---|
| **Cluster #1 (64)** | LT 4, MT 2 | MT 2, LT 4 | LT 2, 3 |
| **Cluster #2 (40)** | LT 1, 3, 4 | LT 1, 3, 4 | MT 1, LT 4 |
| **Cluster #3 (61)** | MT 2, LT 4 | MT 2 | MT 1, LT 4 |
| **Cluster #4 (18)** | MT 1, 2, 3 | MT 1, 2 | MT 1, 2, 3 |

MT: More than, LT: Less than

Table 5
Cluster Analysis by Personality Traits

| **Personality Traits:** | **Extraversion** | **Agreeableness** | **Conscientiousness** | **Neuroticism** | **Openness** |
|---|---|---|---|---|---|
| **Cluster #1 (64)** | LT 2, 4, MT 3 | MT 2, 3 | MT 3 | LT 2, 3 | MT 3 |
| **Cluster #2 (40)** | MT 1, 3 | LT 1, 4 | | MT 1, 4, LT 3 | |
| **Cluster #3 (61)** | LT 1, 2, 4 | LT 1, 4 | LT 1, 4 | MT 1, 2, 4 | LT 1 |
| **Cluster #4 (18)** | MT 1, 3 | MT 2, 3 | MT 3 | LT 2, 3 | |

### *I. Attitude on privacy*

According to [12], public sector biometric usage may be seen as more risky than private sector due to the possibility of state or government abuse. In the absence of proper safeguards, and because of the scale of operations involved, public sector collection of biometric data can be problematic. On the other hand, private sector companies may be more tempted to share or link personal data for marketing or profiling purposes.

To assess privacy concerns about biometrics, one of the survey questions asked participants how trustworthy they thought different public and private institutions were for keeping biometric data private. Business organizations were regarded as the least trustworthy in this respect (only 16% appeared to have confidence in them), while government institutions appeared to enjoy more confidence. This finding appears to contradict the opinion expressed in [12]. However, the fact that no more than 57% appeared to trust the government may be a reflection of the underlying deep-rooted concern people have in general about the protection of their privacy by organizations.

## VII. CONCLUSION

Based on their age, gender, ethnicity and personality, we found no significant differences in the survey participants' perception of the comfort, security and intrusiveness of biometric technology. Opinions varied on the acceptability of individual types of biometrics, but overall, the participants appeared to be more cognizant of this technology, and have a more positive attitude towards it than previously reported. There does appear to exist a significant level of concern regarding the maintenance of biometric data confidentiality by institutions storing such data.

The investigation described in this report used a survey involving male and female subjects who were relatively young. They were graduate or undergraduates university students, and had a mixed background in terms of ethnicity and areas of education (more than 20 different fields). The sample size was bigger than any of the previous studies we had come across. Despite these facts, the subjects are not representative of the population at large in three respects: the distribution of age, levels of education and occupation. As such, the results of this study should be regarded as somewhat limited in its scope, even though many, if not all, of what it highlights as user perception may be indicative of more recent public opinion at large.

A more detailed analysis of the data involving clustering to discover any underlying patterns in users' attitudes based on their personal attributes revealed that participants who were more agreeable and less extraverted or neurotic perceived biometric technology to be least intrusive. On the other hand, those that were least comfortable with this technology tended to be highly extraverted, relatively less agreeable and more neurotic. They also regarded biometrics to be relatively less secure. Participants who were relatively most comfortable with this technology were in general more extraverted, agreeable and less neurotic. This study indicates that a broader analysis of the population at large using available personality characteristics data has the potential to be used as a predictor of public acceptance of this technology of growing importance.

## REFERENCES

[1] B. Miller. "Vital Signs of Identity", *IEEE Spectrum*31(2), pp. 22–30. 1994.

[2] W. Sturgeon. "Biometrics curing password headaches", in *silicon.com*, accessed 19 February, 2011 from <http://www.silicon.com/technology/security/2005/09/28/biometrics-curing-password-headaches-39152802/>.

[3] B. Ngugi, B.K. Kahn, M. Tremaine. "Typing Biometrics: Impact of Human Learning on Performance Quality". In *ACM Journal of Data and Information Quality*, 2(2), pp. 11:1-11:21, 2010.

[4] L. Coventry, A. De Angeli, A., G. Johnson. "Usability and biometric verification at the ATM interface". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, USA, April 5 - 10, 2003, pp. 153-160.

[5] J. Wickins. "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification". In *Science and Engineering Ethics*, 13(1), pp. 45-54, 2006.

[6] A. Chandra, T. Calderon. "Challenges and constraints to the diffusion of biometrics in information systems". In *Comm. ACM* ,48(12), pp. 101-106, 2005.

[7] M. Bromba. "Bioidentification Frequently Asked Questions", in *Biometrics FAQ*, accessed 26 February 2010, from <http://www.bromba.com/faq/biofaqe.htm#Standards>.

[8] NSTC, Subcommittee on Biometrics and Identity Management, 2010. *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards,* accessed 26 February 2010, from <http://www.biometrics.gov/STANDARDS/DEFAULT.ASPX>

[9] A. Sprokkereef, P. de Hert. "Ethical practice in the use of biometric identifiers within the EU". In *Law Science and Policy*, 3(2), pp. 177-202. 2007.

[10] J. Woodward, K. Newton, E. Bradley, D. Rubenseon. In *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns,* RAND Corporation, Santa Monica, USA. 2001.

[11] L. Jones, A. Antón, J. Earp,. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, Alexandria, USA, October 29, 2007, pp. 91-98. 2007.

[12] International Biometric Group, "Privacy Risks in Biometric Deployments: the BioPrivacy Impact Framework" accessed 20 February, 2011 from < http://www.bioprivacy.org/bioprivacy_main.htm>.

[13] S.Furnell, K. Evangelatos,. "Public awareness and perceptions of biometrics". In *Computer Fraud and Security*, vol. 2007, issue 1, pp. 8-13, 2007.

[14] R.Heckle, R. Patrick, A. Ozok. "Perception and acceptance of fingerprint biometric technology". In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, Pittsburgh, USA, July 18 - 20, pp. 153-154, 2007.

[15] Moody, J. 2004. Public perceptions of biometric devices: the effect of misinformation on acceptance and use. In *Journal of Issues in Informing Science and Information Technology*, vol.1, pp. 753-761.

[16] A. Pons, P. Polak. "Understanding user perspectives on biometric technology". In *Comm. ACM* , 51(9), pp. 115-118, 2008.

[17] O. John. S. Srivastava, "The Big Five trait taxonomy: History, measurement and theoretical perspectives". In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research*, pp. 102–138, New York: Guilford, 1999.

**Author Biographies**

**Shamim Khan** was born in Dhaka, Bangladesh in 1955. He completed his studies in applied physics and electronics with an M.Sc from Rajshahi University, Bangladesh in 1979, and earned his Ph.D in computer science from the University of Manchester Institute of Science and Technology, Manchester, UK in 1984. He served as a faculty member at the National University of Singapore from 1984 to 1988 and at Murdoch University, Australia from 1988 to 2006. He is currently an associate professor of computer science at Columbus State University, USA. Apart from biometrics, his main research interests are in the application of soft computing methodologies and decision support systems. He is a member of IEEE, ACM and AAAI.

**Pinar Gurkas** was born in Dusseldorf, Germany in 1974. She completed her studies in psychology with a MA in psychology from Bogazici University, Istanbul, Turkey in 1998. Dr. Gurkas has completed graduate work in applied statistics and earned her Ph.D. in developmental psychology from Purdue University, West Lafayette, IN, USA in 2007. She is currently an assistant professor of psychology at Clayton State University, USA. Her main research interests include relations between environmental contexts and individual differences in human development with particular emphasis on individual differences in temperament and personality.