# What Does the Future Hold for Biometric Technology? A Study into Changing User Perceptions

Amanda Toshack
William Tibben

School of Information Technology and Computer Science
University of Wollongong
Wollongong. NSW
e-mail: atoshack@bigpond.net.au
e-mail: wjt@uow.edu.au

## Abstract

*Biometric technologies have been developed for authentication and verification of individuals. However, expectations of substantial growth in biometric technologies have not been realised. User-acceptance of biometric technologies represents a significant stumbling block to growth. While it is understood that there are different user concerns creating barriers for the industry, the prioritisation of these concerns and how they have changed over time is unclear. This research investigates the changes in attitudes in both the general user and professional user categories that have occurred over the period 1998-2002. Data was generated from both survey and focus group discussion.*

**Keywords**

biometric, user perception, user acceptance, privacy, security

## INTRODUCTION

Biometric technologies have been developed for a wide range of purposes, including authentication and verification. However, the predictions of substantial growth in biometric technology have not been borne out by reality. User-acceptance of biometric technologies represents a significant stumbling block to growth. While it is understood that there are different user concerns creating barriers for the industry, identification of primary user concerns and their significance needs to be better understood.

This paper responds to this problem by reporting on a final years Honours thesis undertaken by one of the authors (Toshack, 2002). The primary goals of the research were to prioritise the main concerns of users in relation to their perceptions of well-being. It was also possible to determine user acceptance of specific biometric technologies and track the changes that have occurred in the period since 1998. Closer scrutiny of these changes indicates that gender specific and age-related issues are at play.

The analysis concludes with an understanding that the study of user acceptance is of value in determining future directions of biometric technology growth. Too often the future is portrayed in terms of the technological dynamic. This research suggests that the machination that occurs in the minds of people is of critical importance. Perhaps of most significance is the finding that there is an interplay between privacy and security which centres on the individuals' sense of well-being

The paper firstly provides a brief background on biometric technology and proposes a model to better encapsulate the numerous concerns that users associate with biometric technologies. The paper then goes on to briefly describe the methodology that guided the study. A summary of the major findings is presented. This summary priorities the major concerns of users and analyses changes that have occurred in relation to peoples perceptions of specific biometric techniques in the period 1998-2002. Of significance is the terrorist event in New York on 11 September 2001 and its influence on the respondents' attitudes. The paper concludes with a discussion that considers the future of biometric technologies and suggests issues for further research.

## BACKGROUND

The medical community has proven that certain human characteristics are unique for each individual. These characteristics can be either physical or behavioural. Physical attributes include DNA (Deoxyribonucleic acid), fingerprints and facial expressions, while behavioural characteristics are based on methods such as signatures or specific keystroke patterns (Borking, Hes, Hooghiemstra, 1999:4). These physical and behavioural attributes have been utilised by engineers to develop biometric technologies for a wide range of purposes, including authentication and verification.

The relationship between user acceptance and the growth of the biometric industry is not a well-researched area. In the years 1995-2000 only a few significant studies have been conducted that focused on predicting and determining biometric growth and examining the results in alliance with user acceptance. Ashbourn (1997 cited in Cowan 1998) states that despite the availability of biometric technology, acceptance on a broad scale has been relatively slow. While it is understood that there are different user concerns creating barriers for the industry, identification of primary user concerns and their actual industry impact is unclear.

## THE STUDY

### User Acceptance and Well Being

In order to gain an understanding of what constitutes user acceptance issues a model was designed to better organize the many issues that are commonly associated with biometric technologies. Issues such as physical contact, religious objections, 'big brother', informational privacy were ordered in relation to three main areas of well-being – spiritual, physical and personal identity. (See Figure 1). The primary purpose of the model was to enable a degree of utility when dealing with the myriad of issues.

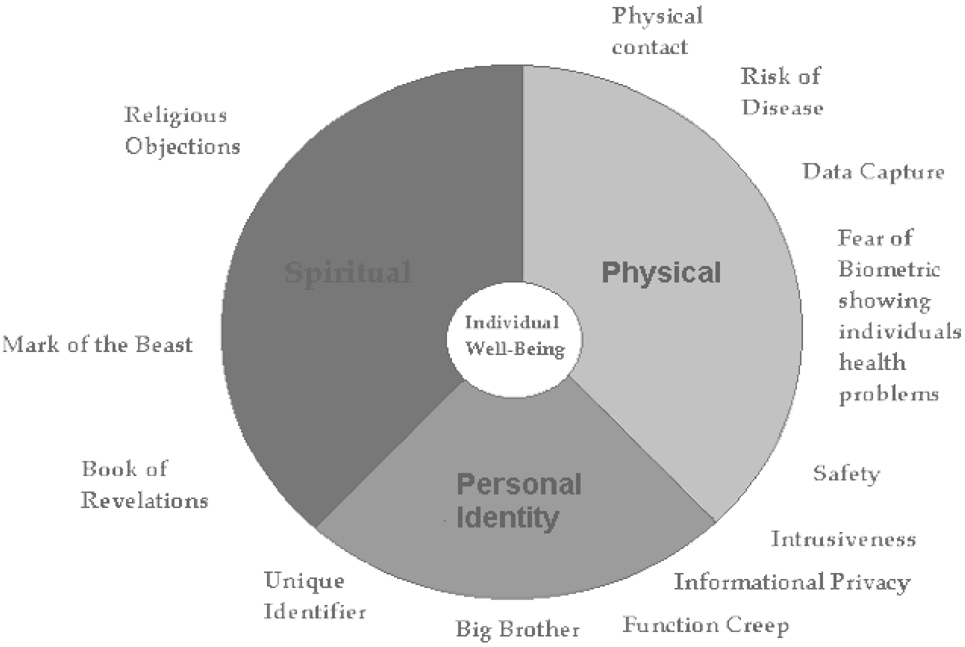

*Figure 1: User Acceptance Issues*

### Physical

Users are concerned about having to make physical contact with surfaces or devices that have been used by others, and hence health and hygiene become acceptance issues for biometric authentication. Woodward (1997) states that this stems from fear of contagious diseases. Rankl and Effing (1997:243) agree, suggesting that individuals are fearful of infection and the infrared beam used in iris scanning. User acceptance of different biometric techniques in relation to issues such as health and hygiene is difficult to assess as it represents a highly subjective measure. However, as with all acceptance issues, particular biometric methods become more of a focal point than others.

### Spiritual

Personal beliefs stemming from religious conviction can be a strong influence on people's use of technologies. Some religious groups believe that biometrics represents the coming of the Apocalypse and fingerprints universally relate to the "Mark of the Beast" mentioned in the Book of Revelations in the Christian Bible (Crowley, 1999:1). Other religious groups state that it is not biometrics that relate to the 'Mark of the Beast', but actually barcodes and biochips (Watkins, 1999:3). For example, Dougherty (1999:1) describes proposed plans to implant biochips into individuals and track their locations via satellites. A The London Times article in October 1998 (cited in Dougherty, 1999:3) argues that several governments will use this information in order to track and monitor individuals.

### Personal Identity

Privacy arguably represents the most controversial aspect of biometric technology. Clarke (2001:5) states that personal and sensitive information can be made available to third parties and interlinked with other information. This provides both public and private institutions the capacity to exercise control over people. Article 5 of the Universal Declaration of Human Rights states that no one should be subjected to degrading treatment (United Nations, 1948). In relation to biometric acceptance, Clarke (2001:8) describes particular uses of the technology, including initial data capture, as demeaning or intrusive to the individual and hence supports the assertion that biometric user acceptance is related to an individual's sense of well-being. User acceptance of biometrics in this context is driven by people's lack of trust in public and private institutuions and the possibility of being monitored.

The degree at which biometric authentication threatens user privacy is proportional to the purpose and context in which users are operating. Certain biometrics engenders a greater public perception of privacy invasion than others (UK Biometrics Working Group, 2002). However, once the data has been captured and stored, the means and techniques used to collect that information are no longer relevant. It is the protection and distribution of that information that become the focus of many privacy debates. Therefore, biometric privacy can be categorised into two (2) areas: physical privacy and informational privacy (Ashbourn, 2000a).

Particular biometric techniques measure unique aspects of the body such as fingerprints, hand geometry and iris scanning. Other technologies focus on varying aspects of human behaviour like signatures, walking style and the process of keying a password as described earlier. Once this information has been captured, it is possible that the biometric may be used to obtain personal information about the user, including medical data, without the individuals consent.

This research therefore aimed to identify the main user acceptance barriers that are associated with biometric technology and to establish any changes to user acceptance levels that have occurred over the past four years. In addition, this research examined the validity of Ashbourn's 'type of user' argument and its affect on user acceptance levels in the Illawarra region. Ashbourne (2000b) argues that by forming a distinction between the different types of users, this will influence acceptance of biometric authentication. Two such distinctions are that of the 'professional user' and the 'general user', with the suggestion that the 'professional' user will be more willing to use biometric technology. A professional user is one who uses the technology as part of his/her job, that is, for example as an Systems Administrator, while a general user is somebody who is required to use the authentication techniques in relation to their working activity or as part of the public system.

## METHODOLOGY

Yin (1994) suggests that to strengthen the validity of research, multiple data collection methods should be used. This research design relied on methodological triangulation. Methodological triangulation involves the use of multiple methods in order to enhance the validity of the findings (Mathison, 1988:1). The two methods employed for generating data in this research were survey and focus group.

The primary data source of this study was a mail-out survey, of which 600 were delivered within the Illawara region in New South Wales. Australia. Ninety people responded by returning completed survey forms. The numbers of surveys and the locality were chosen to provide conformity with a survey that was conducted in 1998. The purpose of the later survey was to identify user acceptance of different biometric techniques. As respondents were required to respond, in part, to identical questions it was anticipated that any changes in attitudes could be determined. Questions pertaining to user attitudes were unique to Toshack (2002).

The survey was categorised into five main areas. These areas included: awareness; levels of acceptance; biometric objections; the effect of the September 11 terrorist event; and personal data. A comments section was also included at the end of the survey, which many respondents utilised to demonstrate their views on topics such as government intervention and privacy.

Section One focused on gaining an understanding of the respondents' level of biometrics knowledge. Section Two concentrated on explaining the different biometric techniques and understanding their willingness to use each method. Section Three presented the respondents with a list of well known biometric objections questioning respondents on which objections they agreed with in relation to specific methods.

The main purpose of Section Four was to understand the impact of the well-publicized terrorist event in New York on 11th September 2001 (9/11) may have had on biometric awareness. Respondents indicated if they were aware of the post 9/11 biometric implementations and their willingness to forego a certain amount of privacy for the advantage of increased security was determined. Section Five provided an opportunity to collect demographic data about the respondent in order to make correlations in regards to certain patterns in age, gender, location and also to cross reference this data with the Illawarra census information to determine if this sample was a true representation of the Illawarra region.

In an attempt to gain a response from a true cross representation of Illawarra residents, 10 districts were chosen and 3 streets from each district received a survey. The demographic makeup of the respondents however, did not exactly match that of the Illawarra population as found in the 1996 Census undertaken by the Australian Bureau of Statistics. There was a slight over representation of female respondents (53.9%) as opposed to the general population of the area (50.3%). Tertiary educated respondents were over represented with 38.4% of survey respondents holding a tertiary education qualification as opposed to the Illawarra census statistics of 21.4%. The 5.4% representation in the 65 years and over group was considerably lower than the 21% found in the general population.

The differences between the general population and the survey sample meant that comparisons between some groupings were not reliable. In relation to gender, the difference was considered to be within limits. Age-related differences meant that some comparisons between groupings were not reliable but findings could be made about proportions within each group. The high response rate from tertiary educated respondents probably skewed responses to a more critical stance on biometric technologies.

Results from the survey and focus group were analysed through a statistical software program, which produced percentages based on the frequency of respondents particular answers. Correlations were also made based on particular patterns within respondents results.

A focus group comprising of four members provided an opportunity to collect data from a secondary source. Bloor et. al (2001:11) support the decision to use a focus group by stating that "focus groups may also be used to interpret survey results, to provide meaning to reports of attitudes or behaviour". Participants for this research were chosen based on their past experience with biometrics and information systems, to allow for the comparison between 'professional' and 'general' users as categorised by Ashbourn (2000c) and to explore the differences in acceptance levels between participants who had never used biometrics before as opposed to those who had prior familiarity.

## PRIORITISING USER ACCEPTANCE CONCERNS

This research identified user acceptance concerns of respondents in relation to biometrics and prioritised these concerns. The purpose of this was to enable a better understanding of which barriers are primarily impacting the biometric industry. In order to prioritise user objections, each issue was given a ranking between 1 and 7, representing most important to least important and the inverse of that ranking was used create a total for that objection. The highest total was deemed the highest user acceptance concern. Table 1 indicates the ranking of user acceptance concerns in regards to biometrics of the survey respondents.

**Privacy** is a topic that features regularly in biometrics literature. This research attempted to identify whether privacy is the central objection associated with biometrics and hence the main issue affecting user acceptance of the technology. The results from both the survey and the focus group indicated that this topic is undeniably the key issue surrounding biometric technology, with privacy being named the issue of highest concern for all biometric methods proposed to survey respondents. Over 64% of survey respondents indicated this issue was among their top three concerns surrounding biometric technology. Focus group participants were concerned about employers being able to access this information and hence build a health profile on employees.

| *Priority* | *User Acceptance Concern* |
|---|---|
| *1* | *Privacy* |
| *2* | *False Rejection* |
| *3* | *Usability* |
| *4* | *Invasiveness of the System* |
| *5* | *Health and Hygiene* |
| *6* | *Religion* |

*Table 1: Ranking of User Acceptance Concerns*

The focus group discussion also reflected a survey finding where a correlation was found between the education level of the respondents and their user acceptance. Those who held a degree or higher degree and those that demonstrated extended knowledge in the field of biometrics, were typically less accepting of the technology. This can be seen through the fact that only 5.9% of survey respondents who held a degree were very willing to try retina scanning, in comparison with 35% of respondents whose highest education level was secondary school. As focus group participants represented a group of knowledgeable users their strong opinions were in accord with the survey findings.

As explained earlier Ashbourne claims that privacy represent two aspects of users' concerns. One aspect relates to physical privacy while the second refers to informational privacy. It was difficult to discern between people's responses in relation to these two aspects – they had a good appreciation of their privacy being violated by eye biometric methods but were also sceptical of how the government uses their personal data. Many respondents stated that rules and regulations need to be developed to govern the use of biometrics. This therefore contradicts a common assumption that knowledge and education per se is the key to lowering user barriers towards biometric technology.

Following privacy, **false rejection** was the next most important user acceptance concern. Many respondents feel that biometrics, specifically behavioural biometrics, are not reliable enough with 30% and 34.4% of respondents indicating that keystroke dynamics and signature dynamics, respectively, are undependable. Ashbourn (2000a:4) concluded that the experience of the user being falsely rejected could create many psychological barriers for the individual towards biometrics, especially if this occurs in a public environment. The high level of concern reflected by the survey results suggests accuracy and reliability of biometric systems needs to be further addressed by developers.

**Usability** was ranked fourth by 25% of respondents. The specific difficulties and concerns that users have in using biometric systems was revealed in the focus group. Participants felt more comfortable using techniques that they had used before and hence understood. This had a direct bearing on their acceptance levels of different methods. Participants had difficulties using speaker recognition and hence this was named as one of the techniques they would be least willing to use. Therefore, this indicates a correlation between the usability of the biometric technique and user acceptance of the method.

The issue of **invasiveness** was a prime concern for biometric techniques such as iris and retina scanning, however, in the context of examining this matter in terms of general biometrics, the objection was ranked fifth overall by 21% of respondents. This suggests that while the issue is a problem specifically for eye biometrics, it is not an overall concern for other techniques. This is supported by the focus group findings, in which participants did not agree that biometrics in general are too forceful, as they prefer the techniques deemed more invasive since they require consent from the individual. 'Consent' was a recurring theme that followed throughout the group's session, with participants preferring biometric techniques in which they were able to make contact with the system "rather than it make contact with me" as one participant stated. The same relationship between user acceptance concerns and eye biometrics was found in relation to concerns of health and hygiene.

**Health and hygiene** was ranked sixth by 38% of respondents. This supports Kim (1995:209) and Miller (1994:27) who state that health and hygiene is a concern for potential users of biometric technology. It can also be seen from this research that this issue typically surrounds biometric techniques that require physical contact, such as finger-scanning, hand geometry, keystroke dynamics and also eye biometrics, like iris and retina scanning. Like usability, this concern seems to centre on eye biometric techniques more so than other methods. Given the high percentage of survey respondents indicating health and hygiene was a problem for iris scanning, retina scanning and facial recognition, the low priority of health and hygiene in terms of ranking was not expected. A reason for this could be that a number of survey respondents agreed with the views expressed by the focus group participants, who stated that touching biometric devices was no different to using other public facilities like shopping trolleys and public transport. Interestingly, participants of the focus group were more willing to try eye biometric techniques than the survey respondents. As the focus group provided an opportunity to further explore reasons behind different responses it appears that participants who wore glasses and visited the optometrist regularly had fewer objections to eye biometrics as they are subjected to eye scans on a regular basis.

The least significant of users concerns was **religious beliefs** with only 3% of respondents stating that this was a concern. Additionally, respondents who indicated that they had religious objections had a high awareness rate and an overall lower acceptance of biometrics. This was unexpected as the traditional pattern suggested that those with a higher awareness rate typically had a high acceptance level of biometrics. This shows that there is a link between religious objections and user acceptance of biometrics, but it only affects a minority of Illawarra residents, as suggested by current literature.

## CHANGES SINCE 1998

Previous research finding developed by Cowan (1998) enabled a number of comparisons to be made in order to understand changes that have occurred in user acceptance of biometric technologies since 1998. As Cowan did not attempt to rank user concerns relative to the individual's sense of well being no comparison in relation to the ranking explained in the previous section is possible. However, it is possible to track changes that have occurred in relation to acceptance of individual biometric techniques.

Looking to table 2 it can be seen that survey respondents display differing awareness of techniques. Particular biometric techniques are more common than others and hence their awareness levels are higher. Over the past four years, the order of familiarity of each technique has not changed, with Illawarra residents still indicating that the biometric techniques of which they are most familiar are finger-scanning, iris scanning and speaker recognition. However, the awareness level of each of these techniques has increased, as was expected due to the overall general increase in biometric awareness.

| ***Biometric Technique*** | ***Awareness Rate 1998 (%)*** | ***Awareness Rate 2002 (%)*** |
|---|---|---|
| *Finger-Scanning* | *65.8* | *73.3* |
| *Iris Scanning* | *65.7* | *71.1* |
| *Speaker Verification* | *61.4* | *65.6* |
| *Retina Scanning* | *56.0* | *62.2* |
| *Facial Feature Recognition* | *55.4* | *51.1* |
| *Signature Dynamics* | *37.5* | *50.0* |
| *Hand Geometry* | *34.2* | *44.4* |
| *Keystroke Dynamics* | *21.8* | *22.2* |

*Table 2: Awareness Rates*

Ashbourn (1997 as cited in Cowan 1998:103) suggests that the awareness rate of a new technology ultimately affects associated user acceptance levels. Awareness of biometric technology has risen in the last four years from 18% to 34.4%. This constitutes a 91% rise in awareness of biometric technologies. Part of this rise can be attributed to the trial implementations of biometric systems at international airports with 13.5% of survey respondents indicating that they were aware that these systems were in place.

The overall increase in biometric awareness did improve the overall acceptance levels of biometrics (see Table 3). This gives support to Clarke's (2001) awareness argument that associated awareness with acceptance. However, this seems to be isolated to physical biometric techniques.

| ***Biometric Technique*** | ***Acceptance Rate 1998 (%)*** | ***Acceptance Rate 2002 (%)*** |
|---|---|---|
| *Finger-Scanning* | 82.5 | 82 |
| *Hand Geometry* | 78.1 | 81.1 |
| *Keystroke Dynamics* | 70 | 66.3 |
| *Signature Dynamics* | 69.5 | 66.7 |
| *Iris Scanning* | 58.5 | 67.4 |
| *Speaker Verification* | 57.9 | 66.7 |
| *Facial Feature Recognition* | 53.5 | 65.6 |
| *Retina Scanning* | 40.1 | 45.5 |

*Table 3: Acceptance Rates*

Methods such as iris scanning, retina scanning, hand geometry, facial recognition and speaker recognition all increased in user acceptance levels by at least 3%, with facial recognition experiencing the highest increase of 12.1%. It could be suggested that facial recognition implementations at airports may have attributed to this rise in acceptance. However, techniques based on behavioural biometrics suffered a decrease in user acceptance over the past four years.

Acceptance of behavioural biometric techniques, such as keystroke dynamics and signature dynamics, decreased 3.7% and 2.8% respectively. This decrease in willingness to use these systems was supported by results of the focus group in which concerns were expressed about the reliability of behavioural biometrics. Reliability was also a concern for 30% of survey respondents in association with keystroke dynamics and 34.4% in regards to signature dynamics. However, in terms of user acceptance concerns, such as health and hygiene, risk of disease and system invasiveness, respondents were more in favour of behavioural biometric methods. From this it can be suggested that reliability is the main objection surrounding behavioural techniques and this may be due to users' lack of knowledge in how these methods operate.

In addition, an interesting developments was discovered in relation to eye-centric biometrics where there was a strong shift in objections towards retina scanning. In 1998, iris scanning was deemed the most unacceptable biometric technique in terms of respondent's concern about eye damage. Just over 56% of respondents cited concern about iris scanning while 49.9% held similar fears about retina scanning. However, in the 2002 survey, retina scanning was deemed the technique that users were least willing to use with 66.7% of respondents stating that they would be concerned about their eyes when using this technique. The level of concern about iris scanning remained relatively static at 57.8%. One explanation for the increase in concern about iris scanning is that increasing familiarity with this technique may have alerted more people to the fact that scanning of the retina requires the user to be situated much closer to the scanning equipment than with retina scanning.

Overall, it can be seen that the user acceptance level of physical biometric techniques have increased over the past four years. A number of elements are attributable to this increase, including the rise in biometric awareness, increased usage of technology (ATM, Internet etc). However, the acceptance of behavioural biometric techniques has not enjoyed such a rise in user acceptance, with its popularity decreasing over the past four years with keystroke dynamics suffering the most. It has not been determined what exactly caused this decrease in these acceptance levels. However, the high concern in relation to reliability identified earlier represents one possible explanation.

## EFFECTS FROM 9/11

A major occurrence that would arguably have contributed to changes in awareness and attitudes to biometric technology was the well-publicised terrorist event in New York on 11 September 2001 (9/11). This was followed by the installation of different biometric systems in international airports, high security organisations and public places such as football stadiums. The deployment of these biometric systems was publicised in the media. As a response, it was expected that 9/11 would have significantly raised user awareness of biometrics, however, this was not apparent in the results.

Only 13.5% of survey respondents were aware that biometrics had been installed in international airports (the most publicised implementation) and only one participant of the focus group knew about the existence of such technologies in these locations. This indicates that the media attention given to the implementation of biometrics as a result of 9/11 was not an influential factor that effected user acceptance levels of biometrics. As a consequence, many respondents needed to be informed about this change in relation biometric technology either through the questions on the survey or by the interviewer within the focus group.

Survey respondents and focus group participants were asked to reflect on the way that their attitudes to biometric technology had changed as a consequence of 9/11. It was discovered that female user acceptance levels were influenced more so by events such as 9/11 than that of males. Evidence for this can be found from the survey results in which 68.8% of female respondents indicated that they are now more willing to use biometrics as opposed to pre-9/11. Even though more males indicated increased awareness of biometrics as a result of 9/11, a smaller proportion of males (58.8%) were more willing to use biometrics. This seems to indicate that females have a higher sense of vulnerability than males in times of crisis and are therefore more willing to accept biometric identification in airports.

The age of respondents was also found to influence user acceptance post 9/11. More so than any other age group, survey respondents between the ages of 55 and 64 years were influenced by the terrorist event. Over 87% of respondents in this age group indicated that the events of 9/11 increased their willingness to use biometric technology.

The majority of survey respondents value their sense of security and safety above personal privacy (81.6%) and are willing to make privacy sacrifices in order to protect themselves from additional terrorist threats (65.6%). This once again supports the assertion that biometric acceptance is related to an individual's sense of well-being. Many respondents stated that while they would forego some privacy in the name of security, they would limit this within the parameters of counter-terrorism. They also stated that they would only permit the use of biometric systems if they have previously been informed of their existence, hence supporting the 'consent' theme of the focus group.

Therefore, the findings of this research show that 9/11 has contributed to changes in the attitudes of respondents. Their awareness and acceptance levels of biometric technologies have increased. When pressed, respondents were also willing to negotiate a lower level of privacy protection within the context of counter-terrorism measures as long as there was a pay-back in terms of increased security.

## WHAT DOES THE FUTURE HOLD?

The randomly sampled population numbered six hundred of which ninety people responded. These preliminary findings indicate a number of interesting features. Most people appear resigned to the understanding that biometric technologies will become more prevalent. Over 97% of survey respondents felt that biometric use will increase. In contrast, only 5.6% of respondents were totally opposed to the use of biometrics. This supports Ferrando's findings from her 2001 research, in which 96.7% of respondents indicated that they feel the use of biometric technology will increase.

Opinions is divided about the factors that fuel user-awareness. Furnell et. al (2000) believe that media coverage is a focal factor in creating this awareness while Sims (1994:14), Kim (1995) and Weber (1998:116) believe common practices within society, such as finger-printing criminals, affect user perceptions. This research project suggests that a number of qualifications need to be employed when considering this question. It is apparent from the survey results that the majority of biometric awareness stems from both news programs and newspapers. The association of criminality with biometric technology is waning in relation to some technologies. For example, in 1998 32% of respondents indicated strong associations of criminality with retina scanning, this had dropped to 7.8% in 2002. Interestingly, the same decrease was not noted in relation to facial recognition where associations of criminality remained relatively static (22% in 1998 and 21.2% in 2002).

An important qualification identified in the literature (Ashbourne, 2000b) and investigated by this research is the type of user. When one views the response of professional and knowledgeable users in the survey and focus group it is apparent that their concerns are factored on rational concerns about their loss of privacy. However, there is little to separate this group from general users who displayed little difference in their acceptance levels even though they had a superficial understanding of biometric technologies. It seems that user psychology is an element that influences user acceptance levels, however the classification of users based on either 'professional' or 'general' use did not appear to significantly affect participants' responses, especially in reference to physical biometric techniques and 9/11. There is an enduring mistrust of those promoting biometric technology be they public or private institutions. The fear of 'big brother' is alive and well suggesting that significant marketing challenges lay ahead for the makers of biometric technology.

However the research did find that within the threat of terrorism most people are willing to negotiate changes to their level of privacy in exchange for greater sense of personal security. This may provide an opening that marketers of biometric technology may wish to exploit. If the introduction of biometric technology can be couched within terms of providing added security less objections are likely to follow. The analysis suggested this when considering the role of the media in informing individuals about biometric technology. While most people identify the media as being their primary source of information only 13.5% of survey respondents were aware that biometric technologies were installed into international airports post 9/11. It appears that if the main thrust of the message is one of security, people may be less likely to associate this with the negative aspects of biometric technology.

The model of well being (Figure 1) developed for the purposes of this research was useful. This suggests that there is potential in refining the concept further for the purpose of developing a framework that is better able to cope with myriad of user-acceptance issues associated with biometric technology. Too often, the predicted success of technology is driven by its technical capabilities. This model has the potential of enabling a more effective inclusion of users when considering biometric technologies.

## CONCLUSION

This paper reports on the findings of a research project that investigated user-acceptance of biometric technologies. User acceptance is considered important because it represents a stumbling block to the deployment of biometric technologies in society. The paper makes progress in addressing these concerns in the following ways.

Firstly, the paper proposes a model of individual well being as a means by which the numerous user-acceptance concerns can be dealt with in a coherent manner. The model was effective in this project and suggests itself as a useful framework for further research.

Secondly, the paper was able to detail the relative priorities that the survey respondents accorded their concerns in relation to biometrics. As expected, privacy concerns ranked first in the minds of a majority of users.

Thirdly, the paper was also able to detail changes that have occurred since 1998 in relation to people's awareness and acceptance of a range of biometric technologies. The events of 11 September 2001 provided an important reference point from which it was possible to determine a greater willingness in respondents to forgo privacy in exchange for greater levels of security.

In conclusion, it can be seen that the increasing penetration of biometric technologies is to some extent inevitable. Many respondents do not like this trend, which indicates a general attitude of negativity across the board from professional users and general users alike. However, it should still be noted that acceptance levels of this technology has increased over the past 4 years and this trend is likely to continue. Overcoming this negativity is a challenge for those who's job it is to promote biometric technologies but if sufficient benefits exist users may feel less reluctant to object.

## REFERENCES

Ashbourn, J. (2000a) User Psychology and Biometric Systems Performance [Online]. Available: http://homepage.ntlworld.com/avanti/home.htm [2002, June 7].

Ashbourn, J. (2000b) Biometric Guru Shares Knowledge [Online]. Available: http://www.precisebiometrics.com/match/nr2/newsline5.asp [2002, August 24].

Ashbourn, J. (2000c) *Biometrics : advanced identify verification : the complete guide*, Springer, London.

Ashbourn, J. (1997) Real world Biometrics [Online]. Available: http://members. aol.com/afb31/af02005.htm [1997].

Australian Bureau of Statistics (1996) *1996 Census of Population and Housing: Basic Community Profile* [Online] Available:http://www.abs.gov.au/ausstats/abs%40.nsf/7c5e80b14f6c2434ca2568b80016b686/d3ade4043a2cfe89ca2568b200194645!OpenDocument [2002, October 16].

Bloor, M. Frankland, J. Thomas M. and Robson, K. (2001) *Focus Groups in Social Research*, SAGE Publications, California.

Borking, J. J. Hes R. and Hooghiemstra, T. F. M. (1999) At Face Value- Biometrical Identification and Privacy [Online] Available: http://www.cbpweb.nl/documenten/av_15_At_face_value.htm- [2002, October, 29].

Bray, H (2002) Reliability of Face Scan Technology in Dispute [Online] Available: http://www.boston.com/dailyglobe2/217/business/Reliability_of_face_scan_technology_in_disputeP.shtml [2002, August 24].

Clarke, R (2001) Biometrics and Privacy, [Online]. Available: http://www.anu.edu.au/people/ Roger.Clarke/DV/Biometrics.html [2002, July 25].

Cowan, B. (1998) User Acceptance Levels for a Home Chip-Card Payment Systems with a Biometric Identifier for Multimedia Service Management, Unpublished Honours Thesis, University of Wollongong.

Crowley, M. (1999) "Identification Technology Raises Privacy Concerns" Las Vegas Review, [Online} Available: http://www.lvrj.com/lvrj_home/1999/Mar-21-Sun-1999/business/10800971.html [2002, October 9].

Dougherty, J. E. (1999) Concern over Microchip Implants, [Online], Available: http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=15185 [2002, May 23].

Ferrando, C. (2001) Biometric Survey Results, [Online]. Available: http://www.dss.state.ct.us/digital/news22/bhsug22.htm [2002, June 24].

Furnell, S. M., Dowland, P. S. Illingworth H. M. and Reynolds P. L. (2000) Authentication and Supervision: A survey of User Attitudes, *Computers & Security*, 19(6), 529-539.

Kim, H. (1995) Biometrics, is it a viable proposition for identify authentication and access control?, *Computers & Security,* 14, 205-214.

Mathison, S. (1988) Why Triangulate?, *Educational Researcher*, March, 13-17.

Miller, B. (1994) Vital Signs of Identity, *IEEE Spectrum – Special Report: Biometrics*, 31(2), 22-30.

Rankl W. and Effing, W. (1997) *Smart Card handbook,* John Wiley and Sons, England.

Sims, D. (1994), "Biometric Recognition: Our Hands, Eyes and Faces Give Us Away", *IEEE Computer Graphics and Applications*, 14(5), Sept., 14 –15.

Toshack, A. (2002) A Comparative Analysis of Biometric Identification Techniques and their User Acceptance Levels in the Illawarra Region, Unpublished Honours Thesis, University of Wollongong.

UK Biometrics Working Group, (2002) [Online] Available: http://www.cesg.gov.uk/technology/biometrics/ [2002, October 9].

United Nations, (1948) Declaration of Human Rights [Online] Available: http://www.un.org/Overview/rights.html [2002, October 26].

Watkins, T. (1999) What about Barcodes and 666? The Mark of the Beast, [Online] Available: http://www.av1611.org/666/barcode.html [2002, May 15].

Weber, J. (1998) Biometric Security, *Australian PC Authority*, April, 114-119.

Woodward, J. (1997) Biometrics: privacy's foe or privacy's friend?, *Proceedings of the IEEE*, 85 (9), 1480-1492.

Yin, R. (1994) *Case Study Research*, SAGE Publications, California.

## COPYRIGHT