Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use

Janette Moody
The Citadel, Charleston, South Carolina, USA

moodyj@citadel.edu

Abstract

Organizations are introducing biometric devices into various sections of the economy for various reasons. What began as a security feature for a limited number of government organizations has been adapted to such diverse uses as paying for school children's lunches to tracking employees' work attendance. From an organizational perspective, justifications for use of biometric devices are plentiful. However, the public's perception of these devices may be quite different. These perceptions in turn will influence public willingness to accept and use biometric devices. Although employee use of biometric devices can be mandated, a more productive alternative might be to understand their perceptions and address those specifically through education and information.

This paper describes common types of biometrics, reviews their current use in organizations, presents findings of a recent survey of public perceptions to determine the areas requiring the most education, and concludes with suggestions for providing this education.

Keywords: biometric devices, computer security, access control devices, employee tracking, information security

Introduction

The term biometrics relates to the measurement (*metric*) of characteristics of a living (*bio*) thing in order to identify it. The techniques of using physical characteristics for identification can be traced to the ancient Egyptians who used the biometric of height (Roberts, 2003). Today the most widely recognized biometric is the fingerprint, which has been in use for over a century. At its inception, fingerprinting required the manual processing of matching between 20 and 7 minutiae points on the whorls, arches, and loops of a fingerprint (Short, 2002). By the mid-1970s, the process had been automated in the US by the Federal Bureau of Investigation into the Automated Fingerprint Identification Systems (AFIS) now used throughout the world (Roberts, 2003). Enabled by the accelerated changes in technological power, other biometrics came to be used, such as hand geometry, iris and retina scanning, voice, and handwriting verification (Harris & Yen, 2002).

Today biometric devices are used in diverse organizational settings ranging from cafeterias for school children (Graziano, 2003) to white-collar employees at the Mitsubishi Motors North America plant (Maher, 2003) to doctors at the University of Arizona Medical Center (Worthen, 2002). The reasons for these implementations are also various. The school cafeteria utilizes the system to track student expenses so that parents only pay for the lunches actually eaten, rather than a lump sum for a full semester. The five hundred Mitsubishi Motors white-collar employees use biometrics to clock in when they arrive at their desks in order to monitor their productivity and time on the job. The doctors have their fingerprints scanned instead of using passwords for logging onto their computer systems, thereby increasing security and saving time in the process. The savings for using biometrics in organizational settings to eliminate passwords and their associated calls to the help desk have been estimated at $50 to $100 per call (Hulme, 2003). When comparing this to the one time cost of current fingerprint scanners of under $100 each (Louwers & VanDenburgh, 2003), the organization's return on investment seems self-evident.

Given the advantages of using a biometric system for monitoring employees and increasing security of information as well as access to buildings, it is not surprising that the industry is expected to grow from $93.4 million in 2001 (Hulme, 2003) to $4 billion in 2007 (Roberts, 2003). However, even with the wide adaptability of the technology to various organizational functions, the acceptance of biometrics has been slow. Reasons cited for hesitancy to use biometric devices include lack of confidence in the reliability, difficulties integrating with other systems, and getting people to change their work patterns (Hulme, 2003). However, the most often cited obstacle is user apprehension (Calderon & Subbaiah, 2003; Fratto, 2003; Roberts, 2003)

Thus, despite these advantages, it has been reported that public perceptions of biometrics can hinder their acceptance. In order to address these perceptions, it is first necessary to identify them. This paper presents the findings from a survey of 300 respondents regarding their familiarity with and acceptance of biometric devices. It begins with a brief discussion of commonly used biometric devices, presents the survey methodology and results, and concludes with suggestions for alleviating misconceptions through education.

Common Types of Biometric Devices

The most common biometric devices used today include: fingerprint scans, iris scans, retina scans, voice recognition, and handwriting recognition. Each will be discussed briefly below. In every case, the initial process for using biometric devices is to enroll the participants in the system by taking several samples of the biometric to be used in order to create a biometric template. The template consists of binary numbers, making it impossible to re-create the biometric sample from the template. This template can then be stored in the biometric reader itself, on a smart card, or in a database (Singleton, 2003) for later use in matching against the enrollee.

Fingerprint scanning can be done in several ways. It can involve use of a silicon scanner that electronically reads the minutiae points on the whorls, arches, and loops that make up a fingerprint, or an optical scanner that takes a picture of the finger, or by an ultrasound scanner that uses acoustic waves to determine the distinguishing characteristics (Calderon & Subbaiah, 2003). Various conditions such as dryness of the skin or dirt and grime buildup on the reader can adversely affect the identification process.

Iris scans are currently in use in major airports in London and Amsterdam, and provide a highly accurate identification process (Staedter, 2003). The identification works by capturing the unique characteristics of the colored ring that surrounds the eye's pupil, consisting of freckles, pits, filaments, etc. These characteristics remain stable over time and are not affected by common surgical procedures, cataracts, or contact lenses. The iris is scanned by simply looking into a video camera about ten inches away for several seconds. This method is considered one of the most secure identity verification systems available (Singleton, 2003).

Retina scans look at the blood vessel patterns on the eye's retina that remain unique for a person's lifetime, but can be affected by cataracts. The scan requires that a low-intensity infrared light be projected through the pupil to the retina (Singleton, 2003), with a 360-degree scan taken to collect data for the reference point template (Harris and Yen, 2002). As with the iris scan, the participant must stand in front of the device for a few seconds in order to have the data captured.

Voice recognition systems create a template of the participant's unique speaking characteristics of cadence, pitch, and tone by having him or her speak preset information into a telephone or microphone (Singleton, 2003). When operational, the system does not require a fixed set of words to verify one's identity but can use similarities in the voice patterns to recognize the individual when unique phrases are spoken. These systems tend to be less expensive and also less reliable.

Hand writing recognition systems collect data that arise from a person's unique writing stroke, rhythm, and pressure flow, thereby capturing *how* the signature was made rather than matching a static image. Although easy to use, a skilled forger can compromise the system and verifications can be hampered by the user's changing physical and mental condition.

Each of the systems mentioned above presents a possible source of concern for participants required to use them. For example, in the case of the retina scan, not only is the projected light considered invasive, so too is the possibility of discernment of certain medical conditions that can be detected by specific patterns of the blood vessels (Singleton, 2003). Some consider this an invasion of privacy that could affect hiring and medical coverage policies. The concept of biometric devices is not new to the public. Biometric devices have been portrayed extensively in movies for some time now and used in a limited way by various organizations, so the public is aware of the devices either by direct contact or by popular culture. Given that the biometrics industry is expected to reach $4 billion in 2007 (Roberts, 2003), it is important to determine what concerns, if any, the public has regarding using these devices, and in what situations they believe their use is warranted. Not surprisingly, biometrics vendors report that the public supports the use of biometrics in various areas (SAFLINK, 2002). The following section discusses an independent survey that was undertaken to look at these public perceptions.

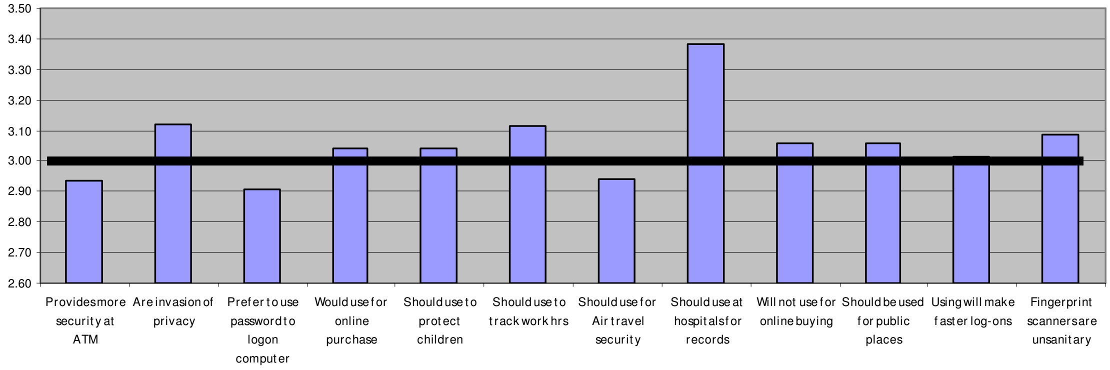
Survey Methodology

It was determined that an independent look at the public's perceptions of biometrics was warranted, based on the vendor's report noted above. Therefore, a survey instrument (see Appendix) was developed which included questions based on a literature review of concerns regarding the most commonly used biometric devices as discussed above. The survey asked the respondent to identify his or her perceptions of these biometric devices, and where the use of these devices would be appropriate. The survey form was given to 15 adult working professionals in the U.S. who were also graduate students in a computer technology class. Each student collected 20 or more survey responses from a random subset of his or her colleagues, friends, family members and/or strangers. The result was a sample of 300 usable responses representing a cross section of the population. The sample consisted of 36% females and 64% males, with 43% between the ages of 21-30 years old, 40% between 31-50 years old, and the remaining 17% either below 20 years old or above 50 years old. In addition to collecting the demographic information noted above, questions 1 through 12 required the respondent to select on a 5-point Likert scale whether they Strongly Agreed or Strongly Disagreed with the statement. Questions 13 through 16 required a forced selection of one or more biometric devices for a given situation, and the remaining three questions were open-ended to collect the respondent's current usage of biometric devices, concerns about biometric devices, and predictions for biometric devices.

Survey Results

The results of the survey illustrate how diverse and even contradictory public opinion is regarding the use of biometrics. Of the 300 respondents, on 6% had ever used one of the biometric devices listed, most commonly to gain entrance to their fitness club or tanning salon. Because of this, respondents often selected the “neutral” or “undecided” answer on various questions. For example, the question “I would prefer that doctors and hospitals use biometrics to guard my records” received the largest number of “neutral” responses at 40%, while 32% “agreed” and “strongly agreed”. The question “Biometric devices provide more security at an ATM” (Question 1) had the lowest percentage of “neutral” responses at 8%, and the highest percentage of “strongly disagree” and “disagree” answers at 49%. Respondents were evenly split on the question of using biometrics for online purchases or protecting school children (40% vs. 40%). Forty-three percent “agreed” and “strongly agreed” that biometrics are an invasion of privacy (Question 2) while only 25% were “neutral”. Figure 1 illustrates the average response on each question.

Figure 1
Public Percptions of Acceptable Uses of Biometrics
(5=Strongly Agree, 3=Neutral, 1=Strongly Disagree)



If required to choose a biometric for logging onto the computer, the majority (53%) would prefer the fingerprint scan (Figure 2), which was also seen as preferable (59%) for use at an ATM (Figure 3) and accessing the office (58%) (Figure 4). Respondents are most uncomfortable using the iris scan (41%) and retina scan (47%) (Figure 5).

Figure 2
Acceptable Biometric for computer logon

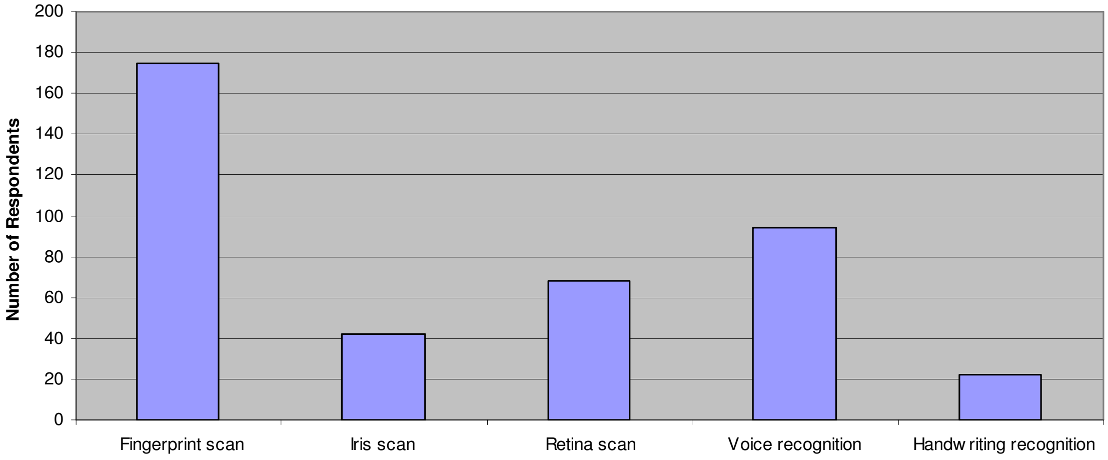


Figure 4
Acceptable Biometric to access office

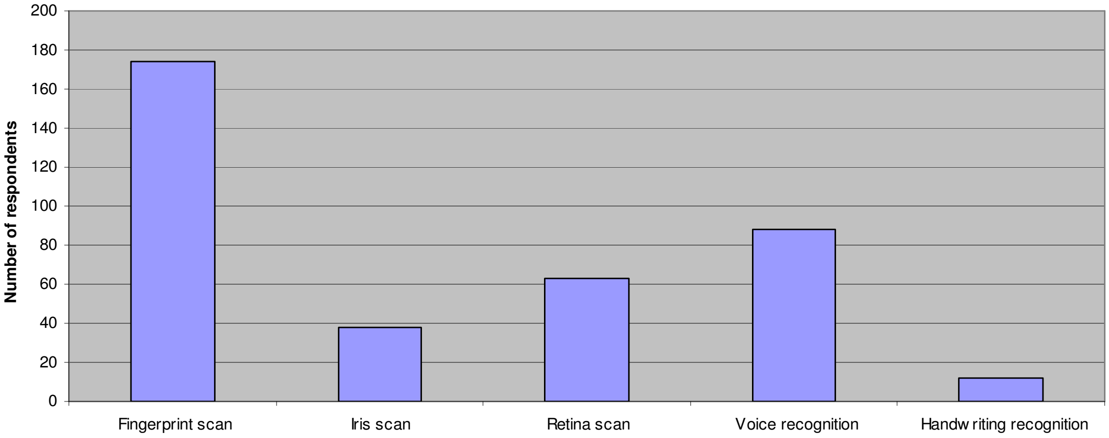
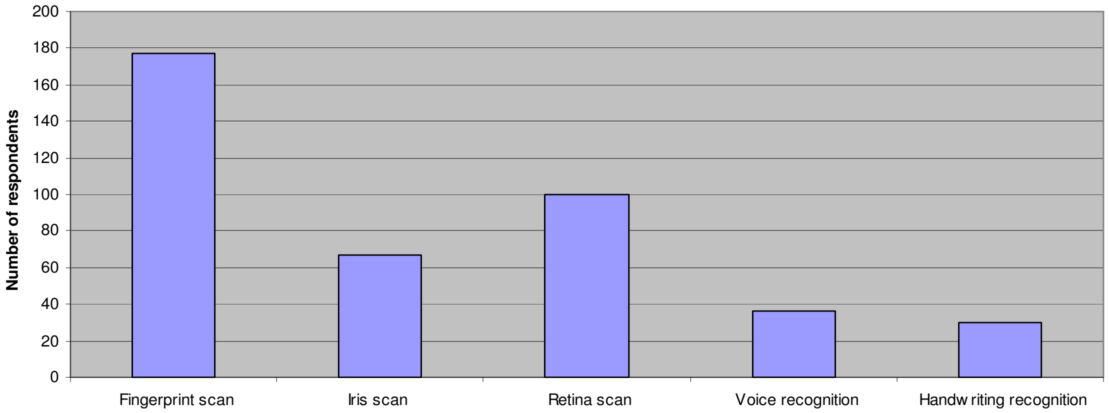
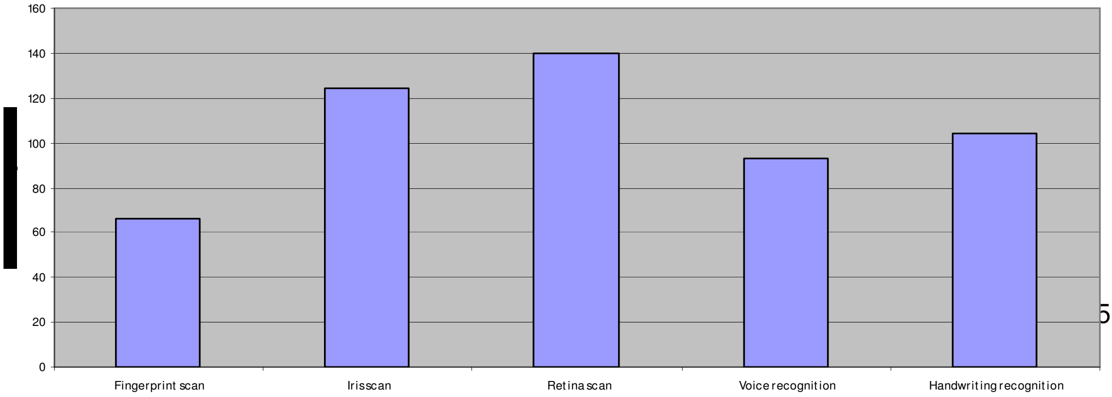


Figure 3
Biometric Acceptable at ATM



When analyzed by age and sex (Table 1), only 6 out of 12 questions resulted in significant differences based on age of respondent. Older respondents are significantly (at p<.05) less likely to believe that biometrics provide more security at ATMs, are significantly less likely to want to use

Figure 5
Uncomfortable using these biometrics



biometrics to order online, significantly less likely to want biometrics to be used to secure medical records, and significantly less likely to think that biometrics will help them log onto their computers more quickly. Older respondents are also more likely to want to keep using passwords to log onto their computers. There were no significant differences on any of the questions between male and female respondents.

Table 1: Correlation Coefficients Based on Age and Sex

Correlation Coefficients by Age and Sex

p significant at <.05 (*p* value indicates the observed significance level (Sincich, 1995,p. 493))

(***r*** value indicates the degree and direction of correlation between the variables (Sincich, 1995,p. 619))

		Age	**Sex**	**Comments**
Q1: Provides more security at ATM	r	-.1661	-.0396	Older respondents significantly LESS likely to agree.
	p	.004*	.499	
Q2: Are invasion of privacy	r	.0877	-.0154	
	p	.130	.792	
Q3: Prefer to use PIN for security	r	.1318	-.0784	Older respondents significantly MORE likely to agree.
	p	.023*	.179	
Q4: Would use for online purchase	r	-.1529	-.0333	Older respondents significantly LESS likely to agree
	p	.008*	.569	
Q5: Should use to protect children	r	-.0760	-.0267	
	p	.190	.648	
Q6: Should use to track work hrs	r	-.0973	-.0725	
	p	.093	.215	
Q7: Should use for Air travel security	r	.0133	.0268	
	p	.818	.646	
Q8: Should use at hospitals for records	r	-.1500	.0330	Older respondents significantly LESS likely to agree
	p	.009*	.572	
Q9: Will not use for online buying	r	.1587	.0181	Older respondents significantly MORE likely to agree
	p	.006*	.757	
Q10: Should be used for public places	r	-.0191	.0075	
	p	.743	.898	
Q11: Using will make faster log-ons	r	-.1245	-.0414	Older respondents significantly LESS likely to agree
	p	.031*	.479	
Q12: Fingerprint scanners	r	.0916	.0382	

	p	.114	.513	

The open-ended questions revealed that most people (94%) were not using biometric devices in any form and that they were concerned about privacy and identity theft (22%). Other concerns reported were the costs associated with biometrics, lack of trust in the reliability of the devices, fear that criminals would resort to "stealing" someone's body part(s) in order to access one's information, and safety concerns about biometric devices that use the eye. Twenty-two percent said they would favor the use of biometric devices for national security, airports, and government buildings, without specifying how such security might work.

Conclusions

This survey reveals that although organizations may be ready to invest in biometric devices to achieve various organizational goals, the survey respondents are not yet ready to embrace them. As with the introduction of any new technology, user participation in the process is essential. When the Philadelphia school system installed a finger scanning system to track hours worked by its maintenance workers, it included the union representatives in the pilot tests (Roberts, 2003). They also removed any stigma attached to using the system by having the supervisors use it as well. Although iris scanning is the most accurate, it is also more costly and as seen in this survey, it is still perceived, as an invasive device that, along with the retina scans, is least preferred.

Organizations deciding to install biometric devices would be well served to survey their employees in advance in order to determine where their misperceptions and apprehensions might exist. Based on this information, an education and familiarization program could be undertaken to specifically address their concerns. Before investing in any new technology, it is wise to determine not only if it is financially and technologically feasible, but also if it is operationally feasible. Things to be considered include whether or not the device will be outdoors where light glare could affect the quality of the scan, how noisy the area might be if voice recognition is to be used, and other practical aspects of the setting. Since no one biometric device fits every situation, research into the most appropriate technology, taking into account the perceptions of the ultimate end-user, is an important first step.

(This research project is being extended into Australia, Canada, and Malaysia to determine if there are cultural differences in public perceptions of biometric devices. The additional research will also include the demographic metric "educational level" of the respondents to determine if there are significant differences in this area.)

References

Calderon, T. & Subbaiah, V. (2003). Automated fingerprint identification systems: What internal auditors need to know. *Internal Auditing*, *18* (3), 15-26.

Graziano, C. (2003). Learning to live with biometrics. Retrieved September 9, 2003 from http://www.wired.com/news/privacy/0,1848,60432,00.html

Harris, A. & Yen, D. (2002). Biometric authentication: Assuring access to information. *Information Management & Computer Security*, *10* (1), 12-19.

Hulme, G. (2003, February 10). Slow acceptance for biometrics. *Information Week*, 56-62.

Louwers, T. & VanDenburgh, W. (2003). Data confidentiality in an electronic environment. *The CPA Journal, 73* (3), 24-27.

Maher, K. (2003, November 4). Big employer is watching. *The Wall Street Journal*.

Roberts, B. (2003). Are you ready for biometrics? *HRMagazine*, *48* (3), 95-98.

SAFLINK (2002). Americans support user of biometrics to improve security at airports and public arenas. Retrieved September 28, 2003 from http://www.saflink.com/62602.html

Short, B. (2002). Getting the 411 on biometrics. *Security, 39* (7), 48-49.

Sincich, T. (1995), *Business statistics by example*. Upper Saddle River, NJ: Prentice Hall.

Singleton, T. (2003). Biometric security systems: The best InfoSec solution? *EDPACS*, *30* (9), 1-24.

Staedter, T. (2003). Iris identification. *Technology Review*, *106* (2), 73.

Worthen, B. (2002). How to meet tomorrow's privacy rules today. *CIO, 19* (3), 1-3.

Biography

Dr. **Janette Moody** received an MBA and PhD in Management Information Systems from the University of South Florida. She received a BSBA degree in Statistics from University of Florida and certification as a Certified Public Accountant (CPA) in Florida. Dr. Moody teaches graduate and undergraduate courses in Management Information Systems, Accounting Information Systems, Project Management, and Software Applications

Prior to entering academia, Dr. Moody worked for Price Waterhouse CPAs, GTE Corp., Eastern Airlines, and Jack Eckerd Corp. Dr. Moody has published articles in numerous journals, including MIS Quarterly, Expert Systems with Applications, and JMIS and is a frequent presenter at both national and regional conferences. Her research interests are in the areas of the behavioral aspects of systems development and the managerial aspects of IS personnel.

Appendix - Biometric Questionnaire

We are interested in your thoughts about the use of biometric devices for gaining access to information and/or physical facilities. Your answers are completely anonymous and will only be consolidated for insights regarding general population views.

Biometric devices are electronic devices that measure some aspect of your physical uniqueness and are used to verify your identification instead of using passwords or PINs. The most popular ones are fingerprint scans, hand geometry, retina scans, iris scans, facial recognition, voice recognition, and handwriting recognition.

Please circle whether you strongly agree or disagree with the following statements:

	Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
1. Biometric devices provide more security at an ATM than passwords or PINs	SA	A	N	D	SD
2. Biometric devices are an invasion of privacy	SA	A	N	D	SD
3. I prefer to use a password or PIN to logon to my computer	SA	A	N	D	SD
4. I would be willing to purchase items on-line if required to use a biometric logon	SA	A	N	D	SD
5. I think schools should use biometric devices to protect children	SA	A	N	D	SD
6. Biometric devices are a good way to keep track of employee work hours	SA	A	N	D	SD
7. Biometric devices should be used for air travel security purposes	SA	A	N	D	SD

8. I would prefer that doctors and hospitals use biometrics to guard my records	SA	A	N	D	SD
9. I would resist buying items online if required to use a biometric logon	SA	A	N	D	SD
10. Biometric devices should be used for security in stadiums and public places	SA	A	N	D	SD
11. Biometric devices can make computer logons faster and more convenient	SA	A	N	D	SD
12. I think using a fingerprint scan is unsanitary and dangerous	SA	A	N	D	SD
13. I would prefer to use (circle any that apply) to logon to my computer	Fingerprint Scan	Iris Scan	Retina Scan	Voice Recognition	Handwriting Recognition
14. I would prefer to use (circle any that apply) to use my ATM or cash a check	Fingerprint Scan	Iris Scan	Retina Scan	Voice Recognition	Handwriting Recognition
15. I would prefer to use (circle any that apply) to gain access to my office	Fingerprint Scan	Iris Scan	Retina Scan	Voice Recognition	Handwriting Recognition
16. I would feel uncomfortable using (circle any that apply)	Fingerprint Scan	Iris Scan	Retina Scan	Voice Recognition	Handwriting Recognition

Please complete the following:

Male____ Female________

Age group: 10-20 _____________ 21-30____ 31-50_____________ 51+______

I currently use the biometric devices in the following ways:

____

My concerns about using biometric devices are:

____

I think we should be using biometric devices to:

____

Thank you!

We appreciate your input!