

Young Adult Perception and Acceptance of Biometric Technology

By

Anthony Allen

Submitted in Partial Fulfillment of the Requirements

For the Degree of

Master of Science

In the

Computer Science and Information Systems

Program

YOUNGSTOWN STATE UNIVERSITY

November, 2012

Young Adult Perception and Acceptance of Biometric Technology

Anthony W. Allen

I hereby release this thesis to the public. I understand that this thesis will be made available from the OhioLINK ETD Center and the Maag Library Circulation Desk for public access. I also authorize the University or other individuals to make copies of this thesis as needed for scholarly research.

Signature: Anthony William Allen

Typed Name, Student Date

Approvals: Dr. Yong Zhang

Typed Name, Thesis Advisor Date

Dr. John Sullins

Typed Name, Committee Member Date

Dr. Alina Lazar

Typed Name, Committee Member Date

Peter J. Kasvinsky, Dean of School of Graduate Studies and Research Date

©

A. Allen

2012

Dedication

I would like to dedicate the work presented in this thesis to my many family members, the Allens, Bericks, Vigoritos, Rupekas, and Eusanios as they have always loved and supported me in whatever I endeavored to accomplish.

I would also like to specifically dedicate this to my future wife, Helena, as she has already been the driving motivation behind each decision I have made involving my career and education.

Acknowledgements

It is my pleasure to acknowledge the leadership and guidance of Dr. Zhang as his passion for teaching young minds and for the advancement of biometric technologies has led me to the successful completion of this thesis. Thank you Dr. Zhang for your encouragement and guidance as this thesis has been an integral part of my graduate education at Youngstown State University.

I would also like to acknowledge Dr. Sullins for his help throughout the entire graduate program as an advisor, a professor, and a leader. Dr. Sullins has helped me to expand my wealth of knowledge in many areas of computer science and I am eternally grateful for all of his time and efforts during my time as a graduate student at Youngstown State University.

I would like to acknowledge Dr. Lazar who has been such an important part of my studies in the field of databases and data mining. Her teachings have provided me the abilities to effectively view and analyze the data discussed in this thesis. I am eternally grateful for her dedication to her students as she continues to make a difference.

Finally I would like to acknowledge and thank Ross Morrone, a fellow student who has been my associate through conception, creation, and execution of the work presented in this thesis. He has been an important part of my successful completion of the entire graduate program at Youngstown State University as we shared and completed many classes together.

Abstract

The ever growing need for more secure forms of identification has spawned many new and improved technologies. These technologies are known as biometric technologies and as they continue to develop and improve, the opportunity for greater personal and national security drastically increases. The problem is implementation and user adoption. As with any science, it is very difficult to gain wide spread adoption and trust from the general public.

If we are going to continue to improve our security measures in this country then biometric technologies need to continue to be developed. The use of biometric technologies has the best chance of accomplishing this improvement. It is imperative that our country looks to implement these ever important technologies as they protect us in countless ways. There is proof of national success in other foreign countries such as India and the U.K. and their implementation of biometric technologies should be seen as a goal for the United States.

With the tragic events of September 11th 2001, one would assume that the United States would already be a leader in implementing national biometric systems. Sadly this is not the case. There are many reasons for the general public, commercial businesses, and/or the United States government to be hesitant on implementing these technologies. These reasons include but are not limited to cost, privacy issues, reluctance and fear of a “big brother government”, information abuse, identity theft, and public perception of inconvenience or hassle.

One would also assume that the younger generations would be much more accepting of these technologies as they show a much higher comfort level and dependency on the internet and technology in general. This may or may not be the case. Therefore, a survey study is conducted to measure the public perceptions and opinions on the use of biometric technologies that specifically targets the young adults, assuming that their altitude would be more influential in determining the development and future of biometric technologies.

The major findings of the survey study are:

- **Basic Knowledge of Biometrics** - It can be concluded from the results in this section that young adults need more education and experience to build trust in biometric technologies. When introduced to the biometric methods, they are familiar with the use of fingerprinting for identification purposes but are generally unaware of any others. The results are encouraging as the participants trust that biometric data is unique (reliable), but they are unsure whether or not the data can be duplicated (secure).
- **Concerns of Using Biometric Technologies** - We conclude that young adults have concerns and benefits that align with their own personal concern before anything else, especially the topic of identity theft. The benefit that biometric technologies can provide great ease and convenience can get overlooked. There are many people that still view biometric technologies as an inconvenience and hassle and these views need to be changed if biometric technologies are going to be increasingly successful in the coming years.
- **Acceptance of Biometrics Used by the Government and Organizations** - In this section we gained some very distinct feelings of the young adult population toward biometric technologies. Some of these feelings could even be applied to the population as a whole as the situations are not specific to age. Generally the young adult population showed in this section that hassle is a concern, they are concerned with the safety of their money, and they are generally accepting of biometric use.
- **Acceptance of Personal Use of Biometrics** - In the personal use section of survey data there are only a couple of significant findings. Findings lineup fairly well with the age group as the participants felt strongest about logging into a computer, and entering their automobile which are generally very important elements to the young adult population.

The information found here would be very beneficial to both computer and car manufacturers who target the young adult demographic as they could possibly add a fingerprint scanner and attract some additional customers.

- **Attitude of Providing Biometrics** - In this section we found that the young adult population is not afraid to provide their biometric information to companies, the government or universities. The one topic that resulted in some push back is the one that involved new born babies. There will always be a stronger push back with a topic that involves infants, as they can't choose for themselves. Interestingly in this section we saw some very strong support of providing biometric information, but there is still the question of how the sample feels about entities that control the information.
- **About the Technology Advancement** - In this section we definitively see that even young adults are skeptical about who controls any biometric information stored in databases. They also are still unsure about the security and reliability of biometric methods. Finally, like any other technology, the amount of time it takes to use biometric information is a critical component as 71% of respondents would wait a maximum of 10 seconds. The government and companies who wish to institute biometric technologies have a lot of work to do to keep advancing the technology in the coming years.
- **Future of Biometrics** - The future of biometrics is promising but will not be successful unless certain aspects are truly taken into consideration. Young adults are believed to be the most willing to adopt technology, but if there is sufficient hesitation from young adults toward the use and trust of biometric technologies it can be assumed that the baby boomer generation and seniors would be even more skeptical. The government and any

corporate entities that wish to implement biometric systems should heavily consider the data presented in these results.

Table of Contents

1) Dedication.....	iv
2) Acknowledgements.....	v
3) Abstract.....	vi
4) Table of Figures	xi
5) Introduction.....	1
6) Biometric Technologies and Their Place in Society.....	2
a) History of Biometric Technologies.....	2
b) The Importance of Public Perceptions of Biometric Technologies	3
c) Future implications of Biometric Technologies	4
7) Public Perception Survey Methodology	5
a) Survey Preparation and Goals.....	5
b) Survey Design.....	6
c) Survey Method.....	8
8) Public Perception Survey Results and Analysis	8
a) Demographics	9
b) Basic Knowledge of Biometrics	14
c) Concerns of Using Biometric Technologies	18
d) Acceptance of Biometrics Used by the Government and Organizations.....	20
e) Acceptance of Personal Use of Biometrics.....	28
f) Attitude of Providing Biometrics.....	32
g) About the Technology Advancement	37
h) Future of Biometrics	41
9) Conclusions of Survey Findings	46
10) References.....	50

Table of Figures

Figure 1: Gender Data.....	9
Figure 2: Age Data.....	10
Figure 3: YSU College Data.....	10
Figure 4: Ethnicity Data.....	11
Figure 5: Education Level Completed Data.....	11
Figure 6: Computers/devices used Data	12
Figure 7: How often a password is needed to login Data	12
Figure 8: Industry of career or Area of Study Data	13
Figure 9: Yearly Income Data.....	14
Figure 10: What do you know about biometrics?.....	15
Figure 11: Of the five Biometric forms listed, most willing to provide?	16
Figure 12: Of the five biometric forms, which is most reliable?	16
Figure 13: I believe that each person has unique biometric information.....	17
Figure 14: I think a person's biometrics can be duplicated.....	17
Figure 15: Primary concerns of using biometrics	19
Figure 16: Benefits of using biometrics.....	19
Figure 17: Biometric use by the U.S. border patrol.....	21
Figure 18: Biometric use at an airport	22
Figure 19: Biometric use by police officers.....	22
Figure 20: Biometric use at large public events.....	23
Figure 21: Biometric use for entering a school or campus	24
Figure 22: Biometric use for identifying welfare eligibility	24
Figure 23: Biometric use to identify a voter's eligibility	25
Figure 24: Biometric use for background checks of employees.....	25
Figure 25: Biometric checks to purchase firearms	26
Figure 26: Biometric use by a retail establishment for customer service	27
Figure 27: Biometric check to open a bank account.....	27
Figure 28: Biometric used to login to a computer instead of a password.....	28
Figure 29: Biometric used for entering a website (no money involved)	29
Figure 30: Biometric used for online shopping (involving money)	30
Figure 31: Biometric used to enter a car instead of keys	30
Figure 32: Biometric used for entering a building, office, laboratory, or parking lot	31
Figure 33: Biometric used for entering the home	31
Figure 34: Willing to release biometric information to a potential employer	33
Figure 35: Willing to let doctor use biometric information to access medical record.....	33
Figure 36: Willing to provide biometric information to obtain a passport	34
Figure 37: Willing to provide biometric information to obtain a driver's license	35
Figure 38: Willing to provide biometric data to obtain a university ID	35
Figure 39: Willing to provide biometric information to open a bank account	36
Figure 40: Comfortable with a hospital taking biometric information from new-born babies.....	37
Figure 41: Biometrics are more secure than traditional methods	38
Figure 42: Maximum waiting time that would be tolerated	39
Figure 43: Feelings toward government control of biometric data.....	39
Figure 44: Feelings toward company or university control of biometric data.....	40
Figure 45: Feelings toward increasing surveillance cameras at public places.....	41

Figure 46: Biometric technology is more secure than it was five years ago	42
Figure 47: Government spending on biometric research should be increased	42
Figure 48: Use of biometric technologies in our society should be largely increased	43
Figure 49: Anticipate the use of biometric technologies will be largely increased	44
Figure 50: What new features would you recommend for the future generations of biometrics technologies?.....	46

Introduction

Imagine a time where we enter our workplace not with a key, but by speaking an entry code read by voice recognition software. Then, in order to access our computer at work we must touch a pad that reads our fingerprint to confirm our identity. We are traveling for work that day, and at the airport we check in with an eye scanner that reads our iris and prints out our boarding pass after identity confirmation. When arriving home from work, we no longer have house keys but rather enter after placing our thumb on a scanner on our front door. How does the idea of this reality make you feel?

This futuristic idea is not far from being a reality. The technology that many recognize out of science fiction movies undoubtedly already exists. You may or may not have already incorporated it into your daily life. If you have, chances are your employer, university or other organization has implemented this identification system in order to protect very important private information, property or processes to the best of their abilities.

Some would say this technology is nothing but increased hassle and inconvenience. However, is it not a major inconvenience when you lock your keys in your car? Or more importantly, is it not true that the inconvenience of having your identity stolen which puts your reputation and all of your money at risk, is immensely greater than having to scan your eye or finger?

One day the security and performance of biometric identification technologies may be lowered to the current levels of having a photo ID or remembering a password. At this time they are innately and immensely superior, because of the unique information they identify. Whether this superior protection is worth the added effort of physical widespread implementation, the increased financial spending, and the difficulty of achieving widespread user trust and

acceptance is still up for debate. These are the aspects still necessary to evaluate by any government or business that is considering utilizing biometric technologies. This study is going to focus on the last aspect of widespread user trust and acceptance.

This thesis will try to answer the question, “what are the current feelings of the young adults toward biometric technologies?” The method chosen to find these answers is to conduct a market research survey, and then analyze the resulting data. There are seven sections that the survey is broken down into:

- Basic Knowledge of Biometrics
- Concerns of Using Biometric Technologies
- Acceptance of Biometrics Used by the Government and Organizations
- Acceptance of Personal Use of Biometrics
- Attitude of Providing Biometrics
- About the Technology Advancement
- Future of Biometrics

The public perceptions interpreted from this data are integral in telling us whether the U.S. young adult population is ready and accepting of the possibility of widespread biometric technology integration.

Biometric Technologies and Their Place in Society

History of Biometric Technologies

Biometrics is a term to describe a characteristic or a process. A biometric as a characteristic would describe an anatomical, physiological or behavioral characteristic. As a process, a biometric is an automated method utilized to recognize individuals based on the characteristics described above [2].

Biometric technologies are by no means a new concept. Although the current biometrics we are familiar with today are much more developed and reliable, the first known use of a biometric for identification purposes was in ancient Egyptian times. They would use hand impressions in clay for identity verification [4]. Over the years the development of other biometric techniques were developed in Germany, France, Czech Republic, Argentina and London [4]. Each country and each scientist that was involved helped the evolution of this incredible technology. More recently, the biggest leap for this technology took place in the 1960's with the utilization of electronics [4]. Electronics and computer processing provided biometric identification with the ability to make "automated checks against a stored reference" [4]. With the power to exponentially cut down the amount of time spent, as well as dramatically increase the accuracy, electronics changed biometrics as it has every other aspect in our lives.

The Importance of Public Perceptions of Biometric Technologies

Just like any other revolutionary technology, there is an adoption period. This adoption period is crucial for any technology. It determines the technologies' overall success and even the possibility of extinction dependent upon the rate of adoption during the adoption period. For example, when compact discs were created, the public adoption period was vital to the medium as it tried to replace cassette tapes. The compact disc technology and those who provided them needed to prove to the public that they were a viable alternative by increasing public knowledge, and earning user trust with product performance over time. This led to the extinction of cassette tapes, and will happen again with compact discs as mp3's continue to replace them.

Certain biometric technologies are already well known throughout the public (ex. fingerprint), and others are less well known (ex. gait, or ear structure [2]). The question is when

and where in their daily lives will the public be accepting of these technologies? Fred Davis's technology acceptance model states that attitudes and perceptions about a technology are instrumental in the decision to adopt technologies [7]. This is the primary reason for this study. "There are multiple aspects involved in a manager's decision to recommend or not to recommend a biometric security solution in their organization – and vendors and managers should be aware that technology adoption often requires many perceived benefits to be present" [1]. The survey conducted here measured the attitudes and perceptions in hopes of foreseeing the current and future possibility of public adoption of widespread biometric technologies.

Future implications of Biometric Technologies

The difficulty in improving public perception of biometric technologies is that the benefits are not tangible. If a household installs a new fingerprint recognition system for entering the house, the security that the system provides is not easily measured or capable of being presented to the user. This is the same with any other implementation on a computer, building, website, financial transactions, etc. Not until a situation occurs where the individual has their identity stolen, has a break-in to their house or numerous other possible security problems would the individual be able to say "If I had an extra security measure on X, would I not have had Y done to me." While the benefits of biometric technologies are still intangible to the public, it will continue to be an exhaustive process of gaining wide user adoption.

The future of biometric technologies can be bright and in turn can improve many aspects of our life including safety, convenience and efficiency. This bright future is primarily dependent on user adoption. Referring to the futuristic idea presented in the introduction, imagine that all of these scenarios employing biometric technologies are real. It is imperative that users imagine the

security, the convenience and the efficiency that they would experience with the inclusion of biometric technologies into their day-to-day lives. As this study and future studies continue to measure user acceptance of biometric technologies, adoption should increase as IT managers, government agencies and the general public are already testing and implementing new biometrics systems. This testing provides the users with essential experience with the technologies which in turn builds trust and understanding. This trust and understanding is ever more important to be in our government if biometric technologies are to thrive now and in the future. Simon McLaren states “On the one hand, U.S. citizens seem to desire the Federal government to take action to increase the general level of security by implementing improved methods of screening and identification of those who represent a threat. On the other hand, Americans have also expressed concerns that such information might be misused by the U.S. Government or government officials” [3]. These concerns have to be soothed if the people of America are to trust the government, providing the government with the ability to increase the security of its people.

Public Perception Survey Methodology

Survey Preparation and Goals

There is an assumption that “older people are generally less likely to adopt technology than younger people” [9]. The relationship between age and technology adoption is believed to be a negative relationship. As age goes up, the adoption rate of technology goes down [9]. This is a very important subset to measure for the overall user adoption of any technology. However, while it is believed that younger people are more likely to adopt or adapt to new technology, this may or may not be true for biometric technologies. Either way the young adult population is

significant, as the population from age 20-29 grew by 22.7% from 2000 to 2010 [6]. Since this segment of the population is growing and its successful adoption of new technologies will be necessary for the success of the technology world. The effect of age on the adoption of biometric technologies was measured with the student population of Youngstown State University as the selected survey sample.

With the sample population chosen, the goals of the survey were three fold. The first goal was to create a survey that effectively measured the knowledge and feelings of the sample toward the use of biometric technologies. The second goal was to attain a sufficient sample, defined by metrics decided as reasonable and attainable by this survey. A sufficient sample was decidedly defined as over 100 respondents, a fair separation of male and female participants (ideally 50% of each), and a majority of participants under the age of 30. It was decided that any data where the respondent was not 30 years of age or younger could be removed from the data and analysis of this research if it met two conditions, 1) if the loss of respondents was not above 10% of the original 143, or 2) the loss of respondents led to less than 100 total respondents. If the respondents under the age of 30 were removed this would provide that 100% of the data was from “young adults” which is ideal for this study. The last and most critical goal was to perform a thorough analysis of the data and to define the current public perception of biometric technologies of young adults.

Survey Design

The survey was developed after a thorough literature review investigation. This literature review was the source for the creation of a long list of possible questions. After evaluating the questions, seven categories were created (not including demographic questions).

The first category is to measure one's basic knowledge of biometrics. In this section we wanted to determine the knowledge of our participants before presenting a formal definition of biometric technology. Questions in this section are general and ask about the individual's knowledge of biometric technologies.

The second category is to measure the individual's concerns of biometric technologies. Included in this section is also a question asking what the individual views as the potential benefits of biometric technologies.

The third category measures the acceptance of biometric use by the government and other organizations. Government and corporate use of the public's biometric information is a sensitive subject for the general public. For this reason it is imperative to include in our survey.

The fourth category measures the acceptance of personal use of biometrics. In this section we wanted to present the participants with questions involving situations in their daily lives. These situations are another section that the general public is sensitive about as it closely deals with their privacy.

The fifth category of questions asks about the attitude of the participants toward providing their biometric data. This is a very important section as every biometric system that could be implemented needs a database of the user's biometric data to function.

The sixth category of questions measures the participants' opinions on the continuing development of biometric systems. To measure how the sample feels about certain situations utilizing biometric technologies can help to develop the technologies to better satisfy the general public, which in turn helps to increase user adoption.

The seventh category specifically asks how the participants feel about the future of biometrics. More specifically the questions in this section asks about the sample's expectations

of biometric technologies. Finally there is a question that gives the participants a chance to write in their recommendations for the development of biometric technologies.

Survey Method

The survey was created and then printed on paper for distribution. The participants were students enrolled in general education classes in order to get a sample with a variety of educational focuses. This would help to ensure the sample better represented the educational and occupational features of the population at large. Possible biases may have occurred from the fact all participants were enrolled in college at Youngstown State University. Education is believed to have a positive relationship with technology adoption. When education is coupled with age the positive relationship is even stronger [9]. It is important to note that the participants in this survey are 100% enrolled in an educational establishment. This sample is still applicable to the general population as it's not able to determine those in the survey who may not complete their college degree, as well as those who may even attain a graduate degree in the future.

The survey and method were then submitted to the IRB (Institutional Review Board) and approved. The participants were required to sign a consent form before participating in the study.

Public Perception Survey Results and Analysis

To keep the findings organized, the data was placed in spreadsheets where statistics, percentages, and graphs could be visualized. These numbers and graphs are presented later in this section of the thesis. The findings will be separated into their respective sections of the survey, starting with the demographic information. Overall there were 143 respondents in the sample, but there were only 9 over the age of 30. Removing the 9 respondents of the 143 meant

only 6% of the total would be lost. The 9 respondents over the age of 30 have been removed for this survey to focus on young adults bringing the total number of respondents for this survey to 134 providing 100% respondents 30 years of age or younger. This number of respondents was more than sufficient to get an adequate analysis of the topics examined.

Demographics

The results provided in the demographics section by the participants were very positive. The demographics provided data that made possible significant patterns and trends. Presented in the first graph, the gender statistics of 53 males and 81 females provided a very well balanced survey. Although 50% of each sex would be ideal, having 40% male and 60% female still provided a successfully balanced survey.

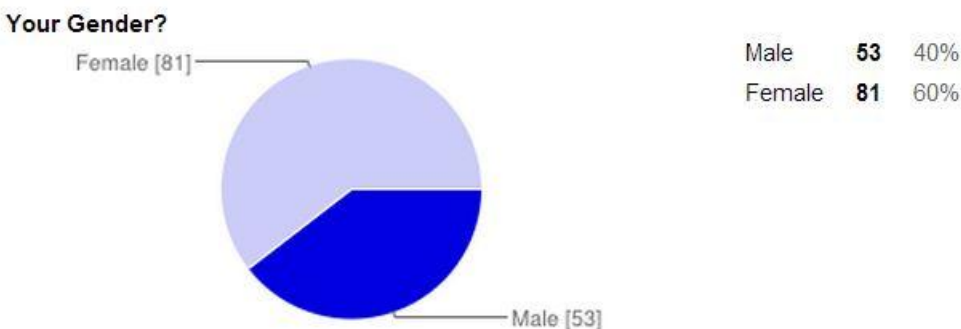


Figure 1: Gender Data

The age demographic was extremely important for testing young adult's perception of biometric technologies. Again there were 9 respondents over the age of 30, but they have been removed from the data to perform this focused analysis. The survey resulted in 82% of respondents between the ages of 18-22, and 18% between the ages of 23-30. The most important fact from this section is that 100% of the survey respondents are 30 years of age or younger which provides much more conclusive results for the study.

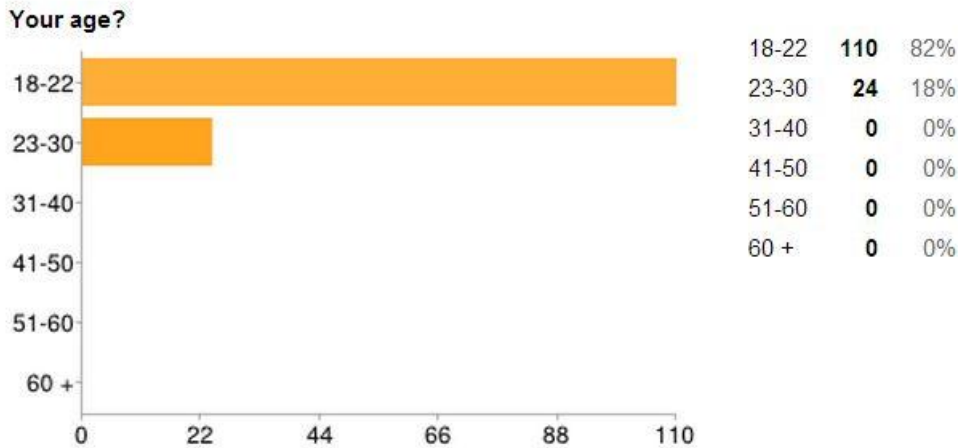


Figure 2: Age Data

This question asks the participants to provide the specific school at YSU in which they are currently enrolled. This breakdown allows for further information about the individuals being sampled. There is a fair distribution of responses in this section. The College of Education is where the small majority of respondents are currently studying followed closely by the College of Liberal Arts and Sciences.

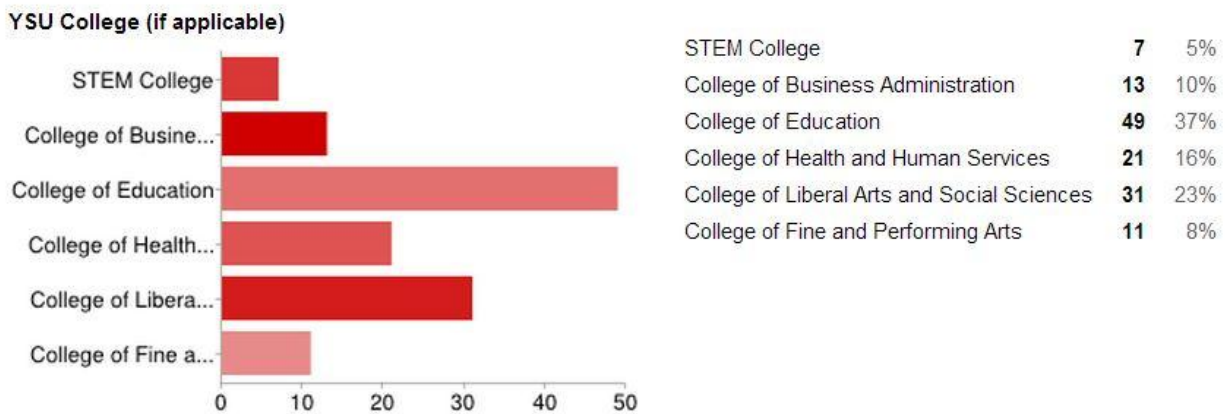


Figure 3: YSU College Data

In figure 4 you see ethnicity data collected. The vast majority of respondents were Caucasian, 82%. It would have been more ideal to have a more distributed sample in this area,

which could have provided a better reflection of the ethnicity breakdown in the population at large.

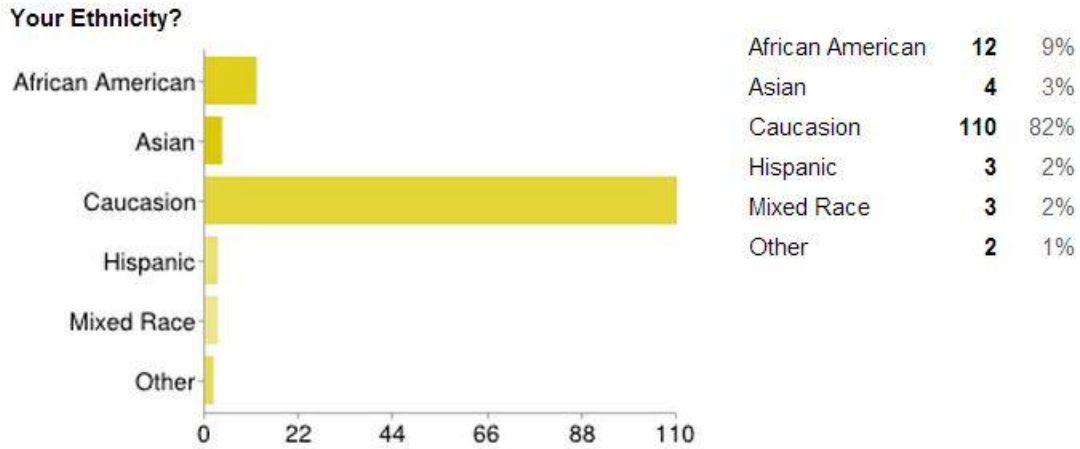


Figure 4: Ethnicity Data

In figure 5 you can see the data on education level completed. As expected 98% of the respondents had either only completed high school, or some college. This is typical for young adults in the population at large, and therefore helps us with the primary goal of measuring young adult’s perception of biometrics.

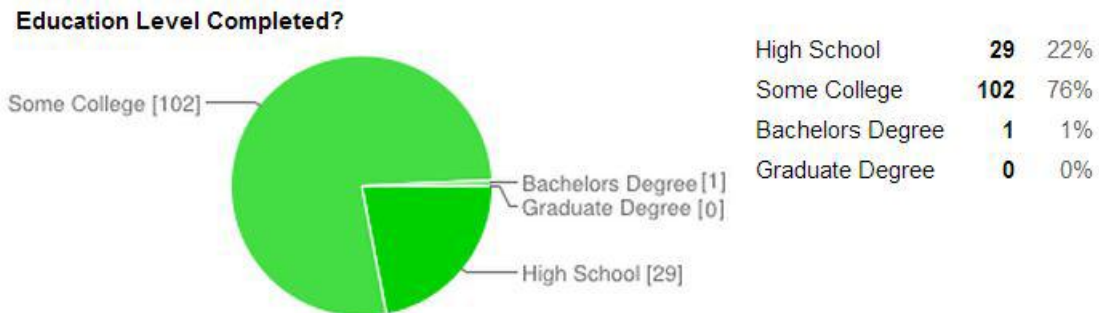


Figure 5: Education Level Completed Data

In figure 6 you can see the types of computers and mobile devices used on a daily basis by the participants. This helps to show that the participants are existing technology adopters of some kind. Primarily the participants use PCs (78%) and an Apple mobile device (54%). A

missed opportunity could have been specifying an option for Android and other mobile users. The alternative may be portrayed in the “other” option where there were 21% of respondents who checked this box.

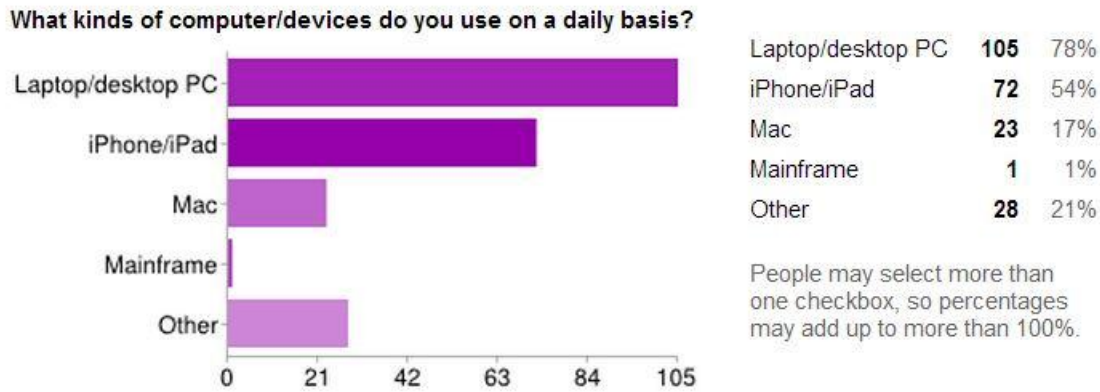


Figure 6: Computers/devices used Data

The data in Figure 7 shows a strong use of passwords by the participants. This also shows that in general the participants use a significant amount of programs or websites where they could be serviced by the use of biometric technology. There are 63% of participants utilizing passwords 1-5 times a day, and another 33% utilizing passwords more than 5 times a day. That means 96% of participants heavily utilize passwords on a daily basis.

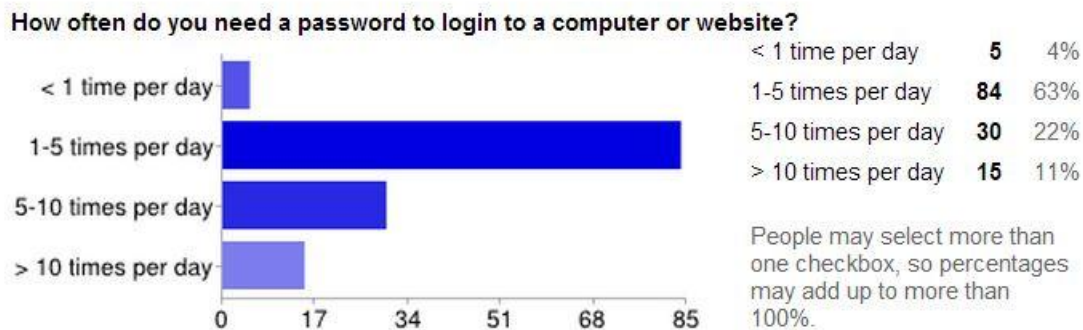


Figure 7: How often a password is needed to login Data

In figure 8 you can see the data listing the industry the participants either work in or study. There might be some confusion here as it may not be known whether the sample works in

or studies in the industry selected. Either way, the participants' primary industry is in education with 35%. This correlates with the previous question that showed 37% of respondents being in the YSU College of Education. There is some evidence of respondents choosing their current employment situation in this question as well as there is 17% who checked retail or food service. These occupations are very common jobs of college students.

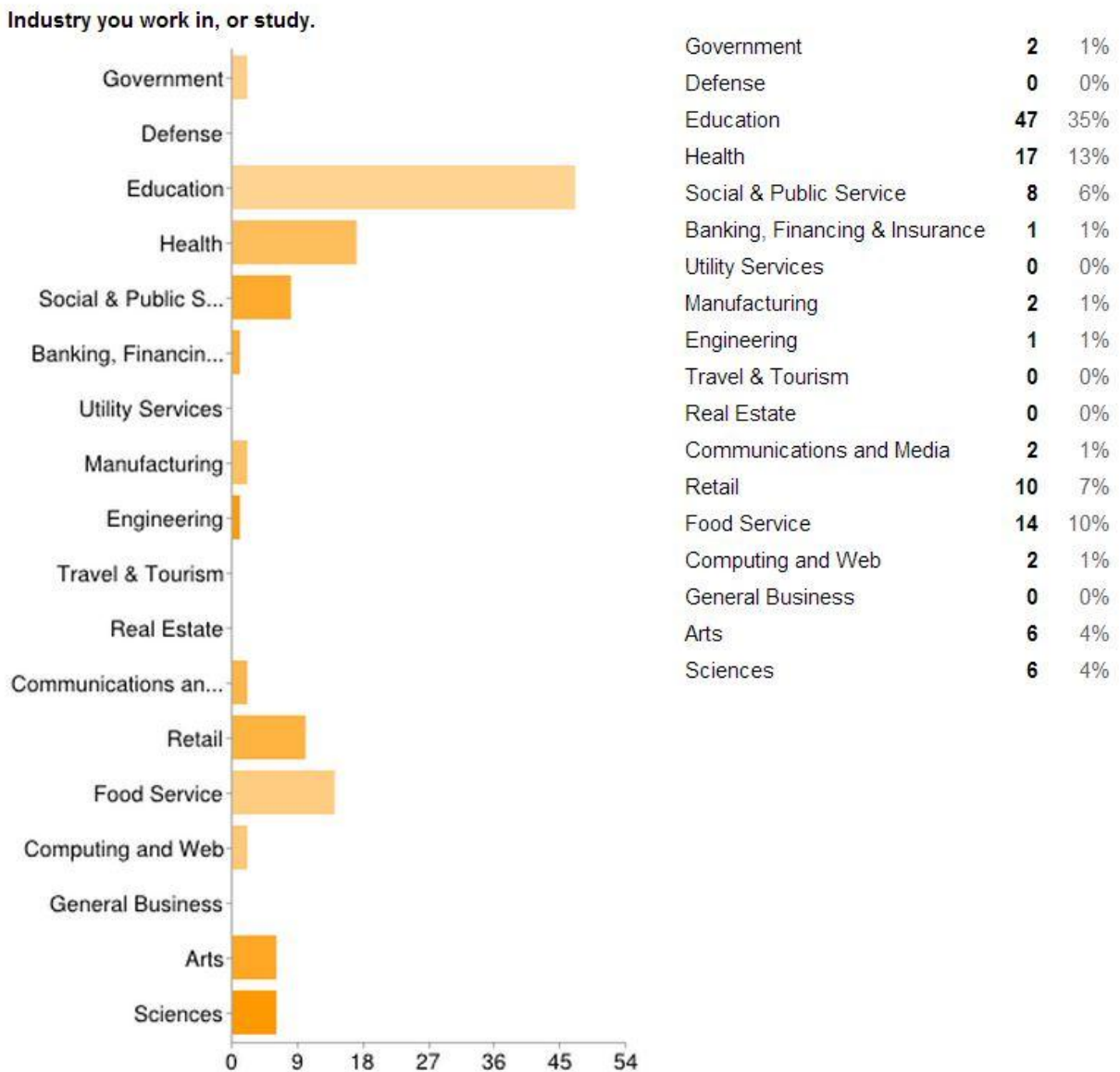


Figure 8: Industry of career or Area of Study Data

In figure 8 there is another correlating statistic supporting the fact that young adults are the vast majority of respondents as 91% of the sample has a current yearly income of \$25,000 or less. One fact to note is that there is some outlying data as 2 respondents answered that their current yearly income is \$75,000 or more. We can't be sure if this is respondent error, respondent negligence or actual data. Never-the-less the data substantially supports the primary study of young college students.

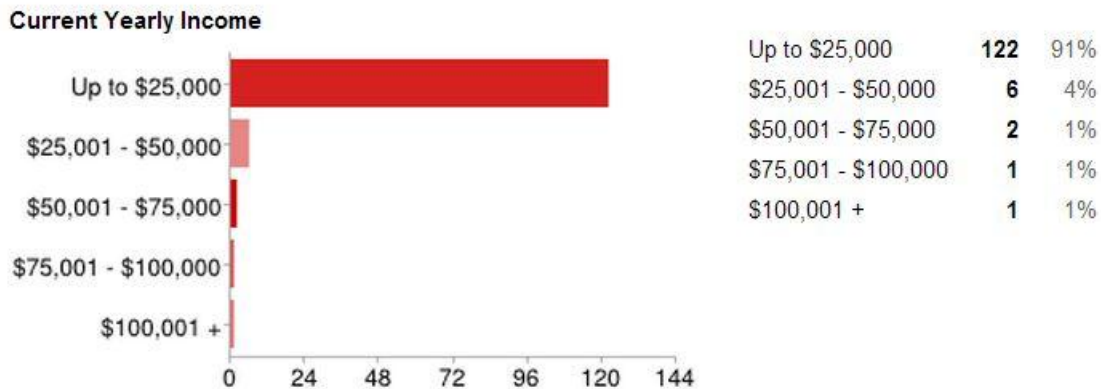


Figure 9: Yearly Income Data

From analyzing the demographic data it can be said the primary goal of measuring young adult's perception of biometrics is indeed intact. There is some outlier data but it is so minimal that the surveys data can be confidently applied to young adults as a whole. Now that the general identity of the sample has been determined, the answers provided in the rest of the survey can be analyzed with confidence.

Basic Knowledge of Biometrics

The second section of the survey measures the participants' previous knowledge of biometric technologies. It is important to establish the participants' knowledge prior to defining biometrics, as previous knowledge and experience can be a prominent factor in adopting

technology. After answering the questions in section two, there is a formal definition of biometrics provided to the respondents for the sections that follow.

Figure 10 displays the data provided by the very direct first question. The first question asked is “What do you know about biometrics?” Here we see that a majority of respondents (54%) stated that they have never heard of the term “biometrics.” This is significant as I pose the question, “how can an individual adopt a technology if they have never heard of it [biometrics] before? The answer provided the second most is “I know a little bit from TV and newspapers” with 27%. Most importantly, the answer of “I have actually used biometric technologies” was only answered 6 times or 4%. There are two variables that have to be true for a respondent to answer the question this way. They have to know what biometrics are, and also have previously used them in their career, in public, or in their personal life. This is a severely low percentage of individuals for any population, especially for the early adopting young adults.



Figure 10: What do you know about biometrics?

In figure 11 is the data from the question, “of the five biometric forms listed, which one would you be most willing to provide?” Here we see that “signature” is significantly chosen most. Second most chosen is “fingerprint.” From these results, it can be concluded that familiarity was a primary factor in the participants’ answer to this question. Familiarity or

experience with any technology can be confidently seen as a factor in a population’s willingness to adopt the technology, and this holds true with biometric technologies as well.

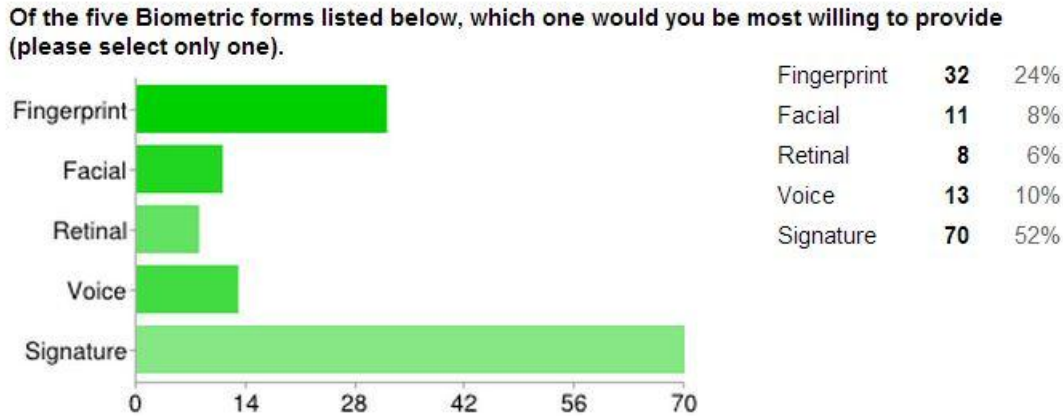


Figure 11: Of the five Biometric forms listed, most willing to provide?

When answering a question, an individual can only answer based on the knowledge they possess. This is why “fingerprint” was the overwhelming choice (61%) when answering the question that is portrayed in figure 12. Education and experience possibly could greatly improve the public perception of biometrics especially facial recognition and retinal scanning.

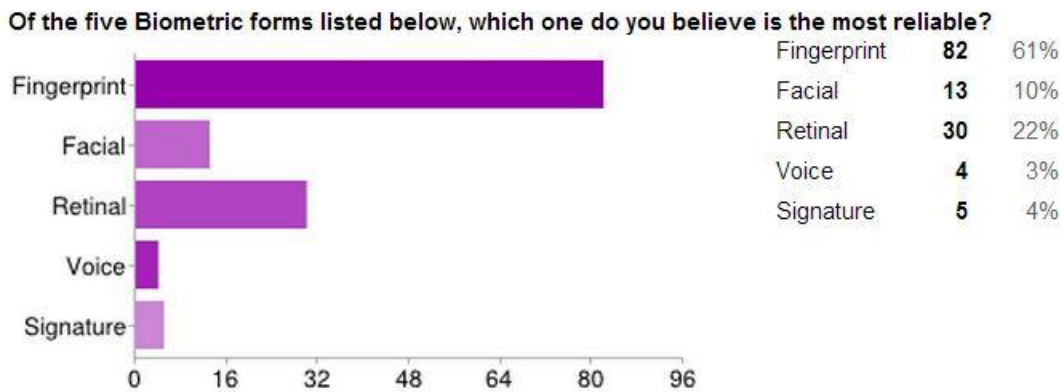


Figure 12: Of the five biometric forms, which is most reliable?

In figure 13 the trust in the uniqueness of biometric data is shown. Here the respondents significantly believe in the uniqueness of biometric information overall with 80% agreeing.

There are 16% of the respondents who were neutral in their trust of unique biometric

information. Continued education of biometric technologies and the use of unique biometric data such as the iris and the fingerprint could help improve the trust portrayed in this data.

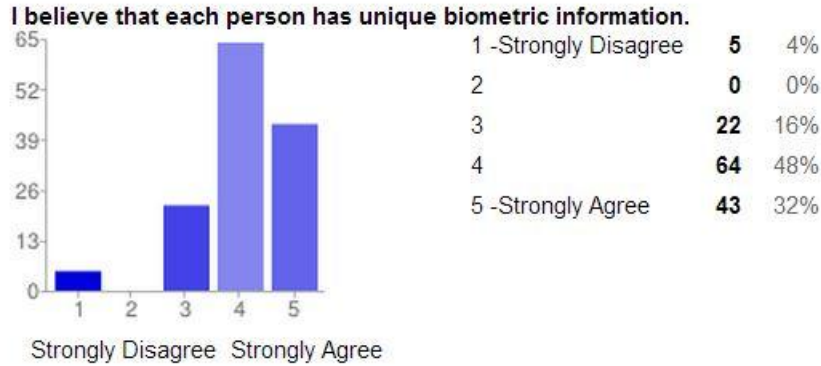


Figure 13: I believe that each person has unique biometric information

Figure 14 shows that the participants were generally lacking knowledge about whether or not biometrics can be duplicated with 46% staying neutral. It is significant that 33% of respondents agreed that a biometric system can be fooled. It is possible to attribute this to media including movies and television shows where spies and criminals can unrealistically defeat fingerprint and retinal scanners with ease. Either way, the government and companies employing these systems should continually assure the general public of biometrics if they want to achieve full user trust.

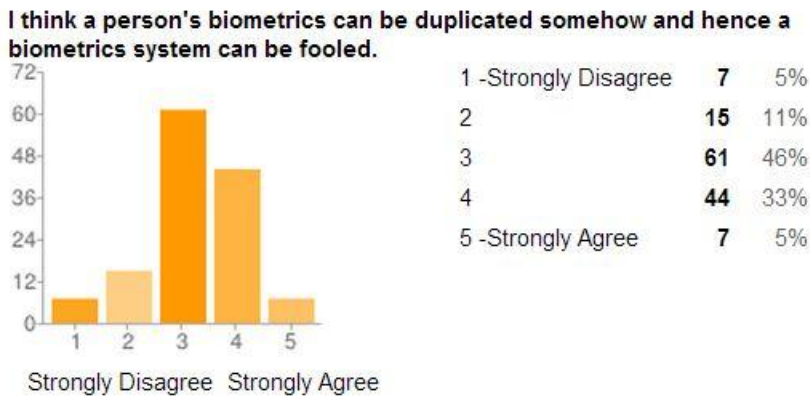


Figure 14: I think a person's biometrics can be duplicated

From the results in this section it can be assumed that young adults need more education and experience to build trust in biometric technologies. When introduced to the biometric methods, they are familiar with the use of fingerprinting for identification purposes but are generally unaware of any others. The results are encouraging as the participants trust that biometric data is unique (reliable), but they are unsure whether or not the data can be duplicated (secure).

Concerns of Using Biometric Technologies

This section is substantially important in measuring the young adult's perception of biometric technologies. Here the survey asked what the respondents felt were primary concerns, as well as benefits provided by the use of biometric technologies. In the simplest form, these are the questions on which people base their choices. Weighing the pros versus the cons is the essential step in any basic decision that a person makes.

The first question asks the respondents to choose their primary concerns in utilizing biometric technologies. Here we find that their primary concerns are privacy invasion and identity theft with 60% and 61% of respondents respectively. In 2002, a paper prepared by ORC International found that (81%) of American adults have heard of identity theft, but a smaller percentage actually knows what criminals do when they steal another person's identity, including using stolen credit cards and cashing forged checks [8]. At this time in America, trust of the government is not as strong as it should be as 46% of respondents checked the "abuse of the personal information by the government. This is a prime example of that mistrust, even among young adults. With identity theft being a heavily publicized subject and everyone growing more dependent on the internet for financial transactions, it is no surprise that identity theft is the leading concern.

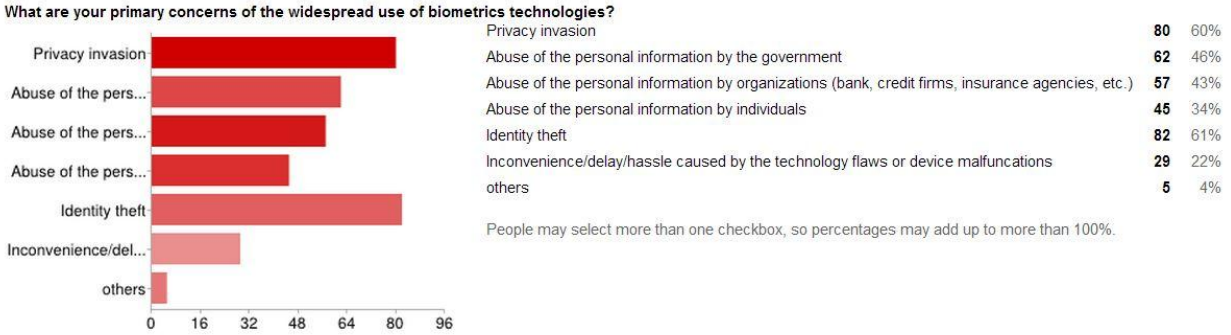


Figure 15: Primary concerns of using biometrics

In figure 16 the benefits of biometrics is chosen by the participants. In correlating with the concern of identity theft, the most popular benefit chosen is “increasing personal safety” with 56%. Although “preventing property damage and financial loss” would relate to identity theft as well, it was chosen fifth as often with 25%. In a close second is “increasing national security” with 53%. This could possibly be a post 9/11 effect, as the general public is still massively concerned with terrorism. Interesting though is the fact that “easy and fast access to computers and facilities” is third with 49%. This tells us that the general public knows this benefit is a possibility, although it will be discussed in a later section whether or not they would feel strongly about choosing to use biometric technologies for this purpose.

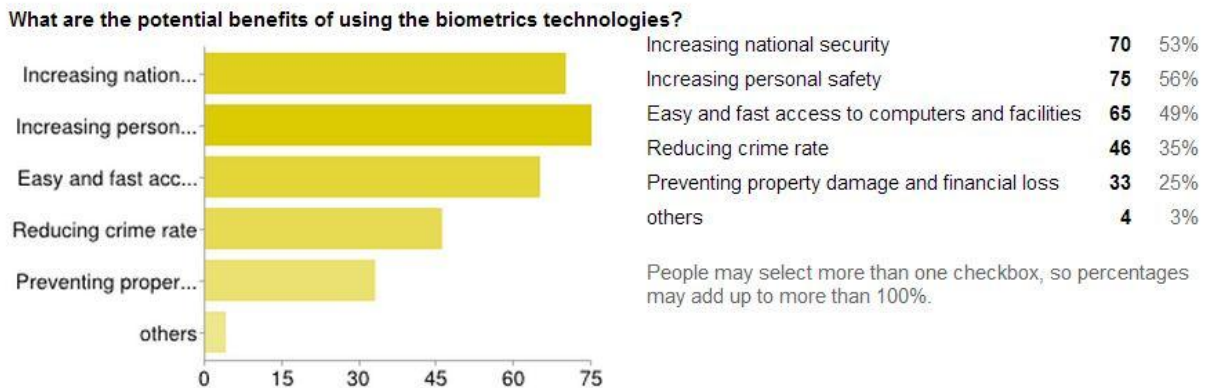


Figure 16: Benefits of using biometrics

It can be concluded that young adults have concerns and benefits that align with their own personal concern before anything else, especially the topic of identity theft. The benefit that biometric technologies can provide great ease and convenience gets overlooked. There are many people that still view biometric technologies as an inconvenience and hassle and these views need to be changed if biometric technologies are going to be increasingly successful in the coming years.

Acceptance of Biometrics Used by the Government and Organizations

In this section the participants were asked questions that involved government or organizational use of biometrics. If there is going to be a national biometric system implemented, we may have no other choice but to comply. This doesn't mean that the government can just ignore the public perception of the technology or the public's rate of adoption. Within organizations, biometric technology can greatly improve security as well as customer service, but the real question is will the employees or customers become comfortable with the changes?

One concern of both the government and the public is the amount of illegal immigrants that come into the United States looking for work and a new life. The influx of immigration is responsible for assuming certain jobs that would otherwise be taken by U.S. citizens; therefore there is concern by many for stricter border control. Figure 17 shows that 58% of participants agreed biometric technologies should be used by the U.S. Border Patrol to improve identification procedures for those crossing the border. There are also 31% of respondents who remained neutral on this question. This high level of neutrality could possibly be a result of the fact that Ohio residents are unfamiliar with the presence of illegal immigrants to a large extent.

There should be a mandatory use of biometric identification systems by the U.S. Border Patrol.

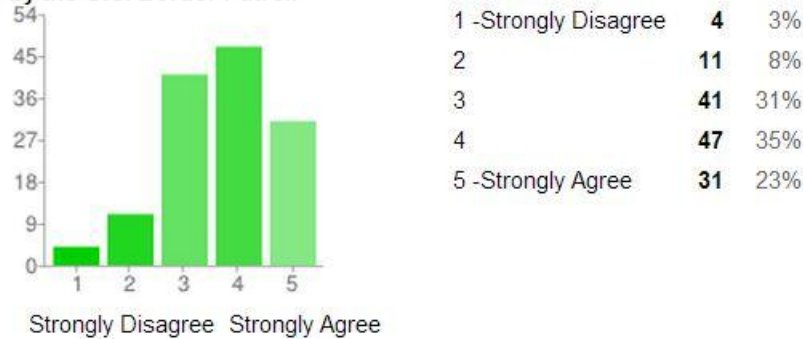


Figure 17: Biometric use by the U.S. border patrol

Our post-9/11 society has seen airport security increase dramatically. It is likely that the use of biometric identification systems can greatly improve not only the security but even the time it takes to go through security at the airport. Figure 18 displays that 55% of respondents agreed that airport security should employ biometrics. There were still 46% or respondents who disagreed or remained neutral on this question, which could be attributed to the public's perception that the implementation of biometric systems at the airport would increase the amount of time going through security. If biometrics were to be integrated into airport security, it is possible there would be some public pushback at first, but with some assurance through media as well as experience with the security the public would probably start to accept the integration of the technology into airport security. It can also be said that biometric technology use at airports is a huge gateway opportunity for getting the public to use the technology and get comfortable with it, therefore building trust of the technology. This is because the majority of the population flies to travel so they would all gain some experience, as well as the high media priority of airports and their security by media which will help to build reputation and trust of the technology as well.

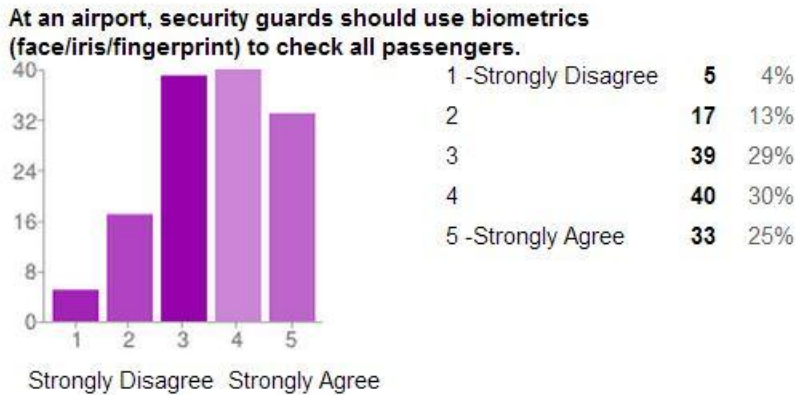


Figure 18: Biometric use at an airport

In figure 19 the feelings of young adults toward biometric use by the police force are shown. This question shows a very similar range of answers but a little less supportive as 49% of respondents agreed with this given situation. While 51% of the respondents remained neutral or were against this situation. This is most likely linked to the extra hassle that would come with being stopped by a police officer on the road. This situation generally brings up negative feelings in the population as a whole; therefore the stronger pushback can be attributed to this notion.



Figure 19: Biometric use by police officers

Figure 20 shows the feelings of young adults toward the use of biometric systems to check people who attend a large public event. In this question there is an even stronger disagreement with this situation than situations in previous questions. There are 34% who

disagree compared to 32% who agree with biometric use at large public events. Maybe the young population doesn't see the need for such a system at large public events because they don't want hassle when attending football games. There is also 34% who are not sure about biometric use for this situation. I would say again that the fear of hassle is the culprit for the disagreement in this data.

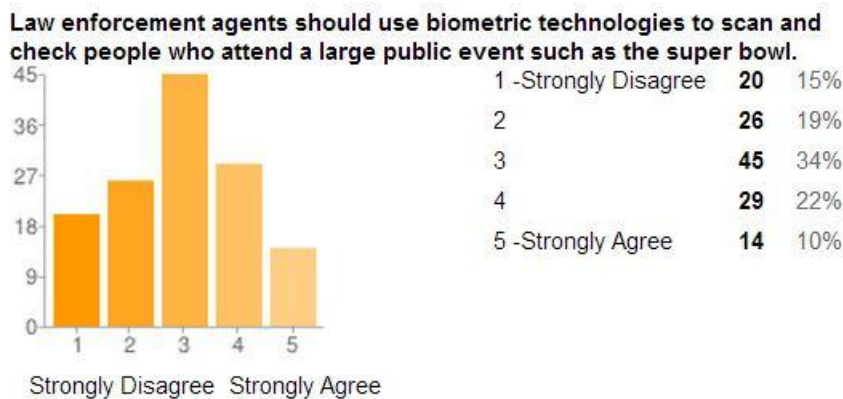


Figure 20: Biometric use at large public events

Figure 21 shows the results of “At a college or high school, the administration could use a biometric method to screen people entering the campus for security reasons. The fact that the sample is 100% college students provides that 100% of the respondents have a direct connection to this question. In figure 21, 39% of respondents agreed that biometric technologies should be used to enter a high school or college campus. The school shootings and incidents of recent years could also be a strong factor in this data.

At a college or high school, the administration could use a biometric method to screen people entering the campus for security reasons.

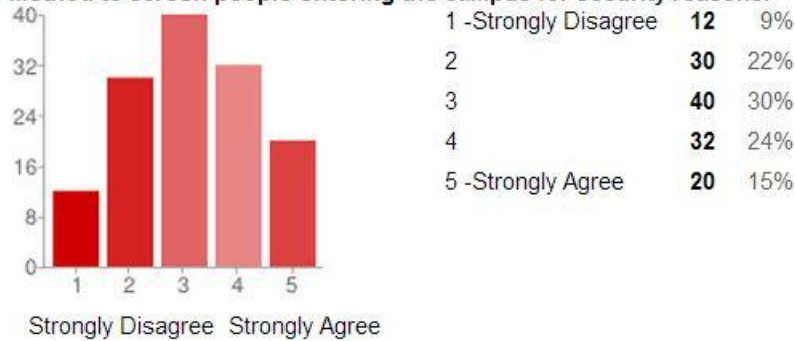


Figure 21: Biometric use for entering a school or campus

In figure 22 is the data of those who believe biometric technologies should be used to identify those who are eligible for welfare. This question has particularly interesting results. 70% of respondents agreed with biometric use in this situation. This can be attributed to the fact that young adults are very concerned about their money, especially college students. In Ohio college students are not eligible to apply for welfare so the only likely experience these students have with welfare is through their parents. This fact may have had an influence on the results.

Welfare managers should use biometrics technologies to check the identity and the eligibility of certain people who attempt to seek double welfare benefits.

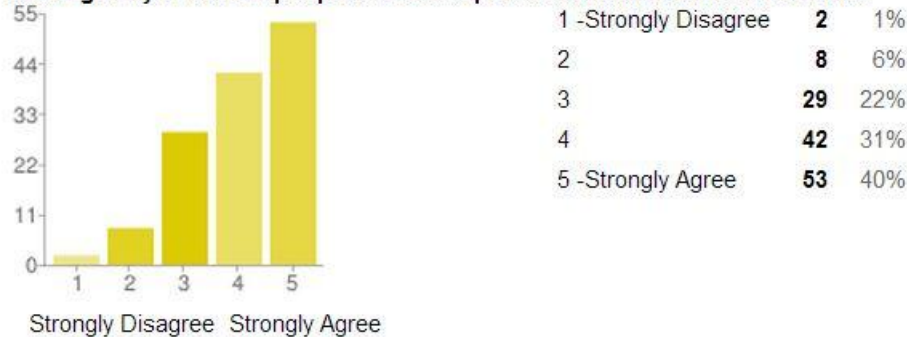


Figure 22: Biometric use for identifying welfare eligibility

In figure 23 are the feelings of the participants toward biometric technology being used to check a voter's eligibility. At the time of this survey, the 2012 presidential election just occurred. It can be assumed that the 34% of people who remained neutral on this question are concerned

with the hassle that comes with voting in general, as well as the possible increased hassle by an extra security measure. Again the possibility that biometric identification could improve the speed of the voting process would not be apparent to all in the survey sample as they have so little experience with the technology.

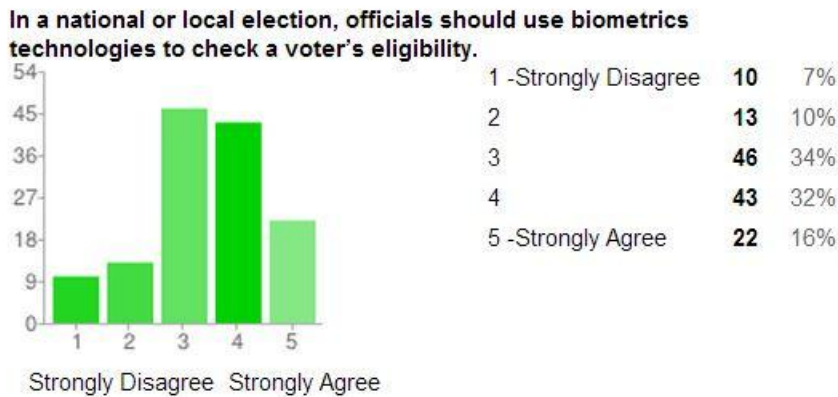


Figure 23: Biometric use to identify a voter's eligibility

In figure 24 are the results to the situation of government agencies using biometric technologies for background checks of licensed workers. An overwhelming amount (82%) of respondents agreed that biometrics should be used for background checks. With the publicity of many abusive situations by workers including teachers, nursing home workers and police officers it is not surprising that the respondents felt so strongly about this situation.

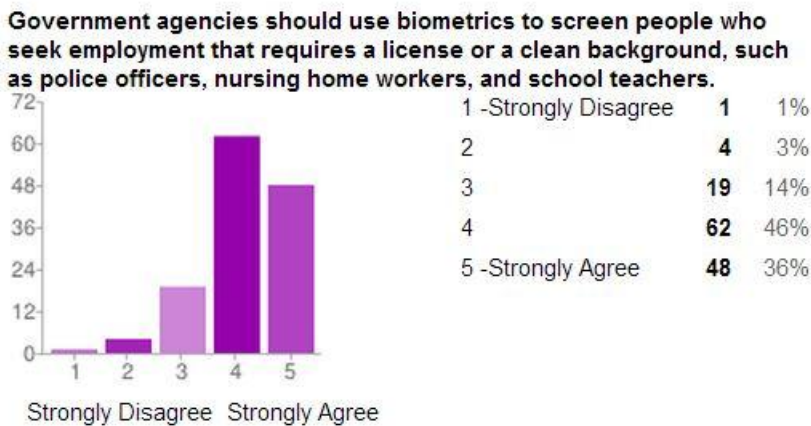


Figure 24: Biometric use for background checks of employees

The results in this question are encouraging. In figure 25 there is an overwhelming response that agrees with the use of biometric checks for people who want to purchase firearms (78%). This is an easy one for the young adult participants to agree with again because it is unlikely the majority of them have bought or even shot a gun. The fact of recent massive shootings over the last few years also would greatly affect the way the population as a whole feels about the purchase of guns. Biometrics could definitely improve the process of purchasing guns in many ways, and it is so important that the public knows this.

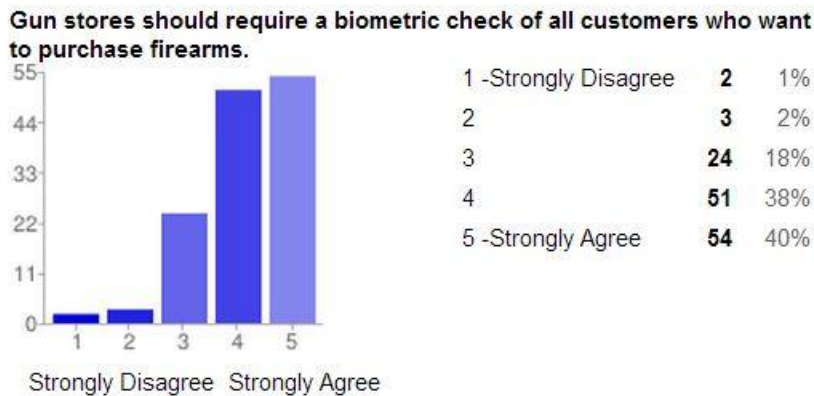


Figure 25: Biometric checks to purchase firearms

In figure 26, a very strong response is shown. The participants greatly disagreed with corporate retail use of biometric information for improvements in customer service (71%). Only 8% of respondents agreed with biometric use in this situation. I would think that hassle again plays a very heavy part in this data. The fact that Wal-Mart is included in the question, and the negative view that some people have about that specific establishment could also affect the results provided. Based on the results it is very likely that the young adult population does not trust corporate establishments with their purchasing data.

A superstore such as Wal-Mart should use a device to scan your face when you pass through the checkout counter. The store will use the information to provide better customer service such as a personalized shopping experience.

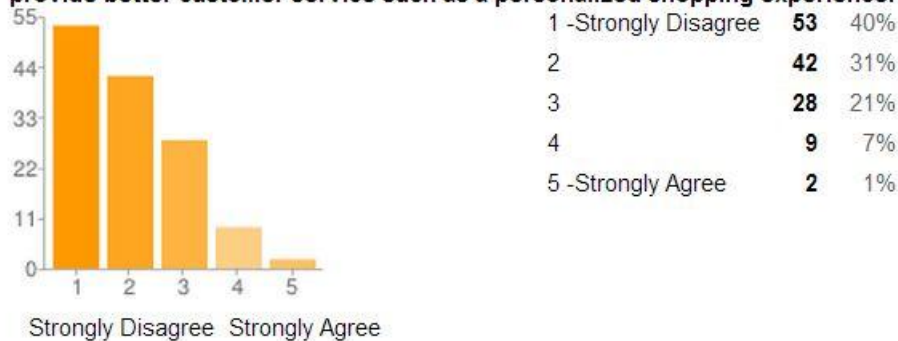


Figure 26: Biometric use by a retail establishment for customer service

In figure 27 is the participants’ response to requiring a biometric check to use credit cards and ATMs. 52% of the population agrees with biometric use in this situation. 33% of those respondents only agree, and do not strongly agree. It can be assumed that hassle again plays a part in this hesitation. It can also be assumed that the risk of personal safety and identity theft is a driving force in the respondents’ responses to this question.

In addition to the PIN, banks should require a biometric check for using credit cards and ATMs.

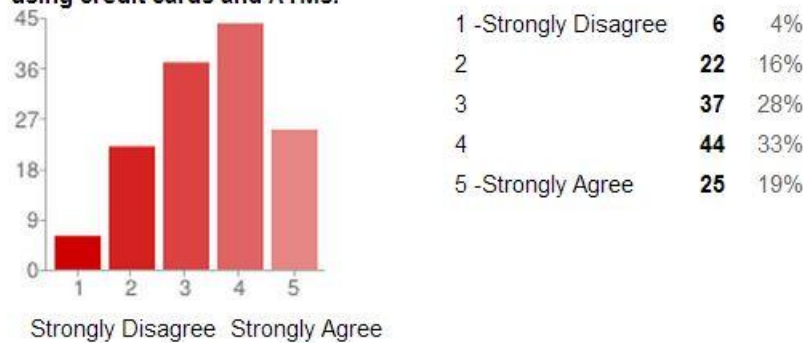


Figure 27: Biometric check to open a bank account

In this section there are some very distinct feelings of the young adult population toward biometric technologies. Some of these feelings could even be applied to the population as a whole as the situations are not specific to age. Generally the young adult population showed in

this section that hassle is a concern, they are concerned with the safety of their money, and they are generally accepting of biometric use.

Acceptance of Personal Use of Biometrics

Personal use is an entirely different situation that the public has to adopt for any technology. Biometric use in the population's daily lives is going to take some time to gain widespread adoption compared to using it at public establishments such as airports or the grocery store. In this section the goal was to measure the young adult participants' view toward the use of biometrics in their personal lives.

The first question asked the participants how they felt about using a biometric to login to a computer instead of using passwords. It is generally known how unreliable a password can be for security. Another flaw in the use of passwords is that they can be forgotten, which leads many people to write their passwords down on paper, sometimes that is right next to their computer. In figure 28 it is shown that the respondents generally were in favor of using a biometric to login to their computer (44%) compared to 28% who disagreed and 28% who were neutral.

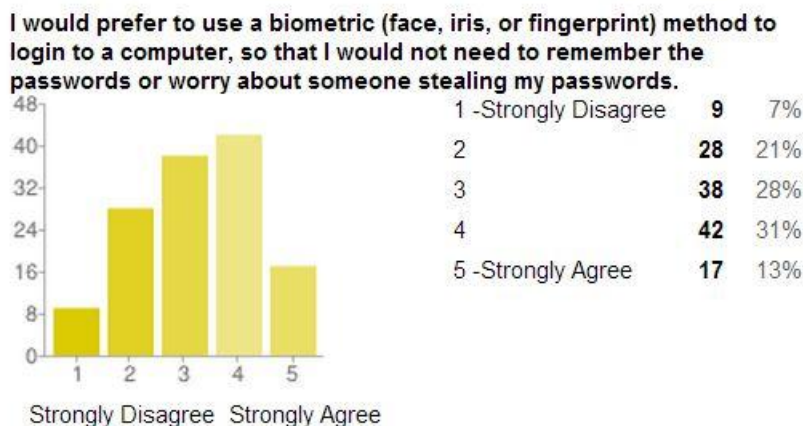


Figure 28: Biometric used to login to a computer instead of a password

The second question in this section provided data on whether or not the participants would like to use a biometric method to login to a site on the internet. The results are very even as 37% of people would prefer to use a biometric, and 36% would not prefer to use a biometric. They could have answered this way for a couple of reasons, 1) so many websites are visited each day and no one wants to scan their thumb to enter every website, and 2) this question strictly says that no financial activities are involved so the question doesn't provide that extra motivation to make their online transactions secure.

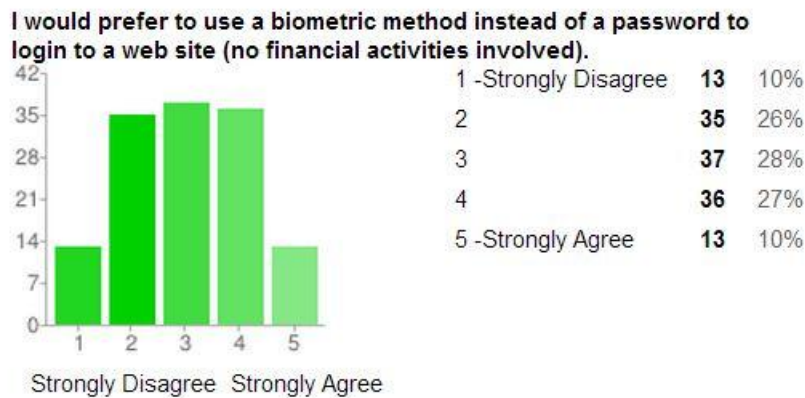


Figure 29: Biometric used for entering a website (no money involved)

In figure 30 are the results to the next question, “I would prefer to see a biometric method instead of a password to do online shopping (involving money transaction). The respondents were slightly more agreeable. The specific mention of money transactions could have affected this. In figure 30 it is shown that 37% of the respondents would prefer to use a biometric method compared to 33% that would not prefer it. The neutral percentage also went up 1% to 29%. It can then be assumed that the young adult population is not convinced that biometric technologies would be able to drastically increase the security on financial activities completed on the internet.

I would prefer to use a biometric method instead of a passwords to do online shopping (involving money transactions).

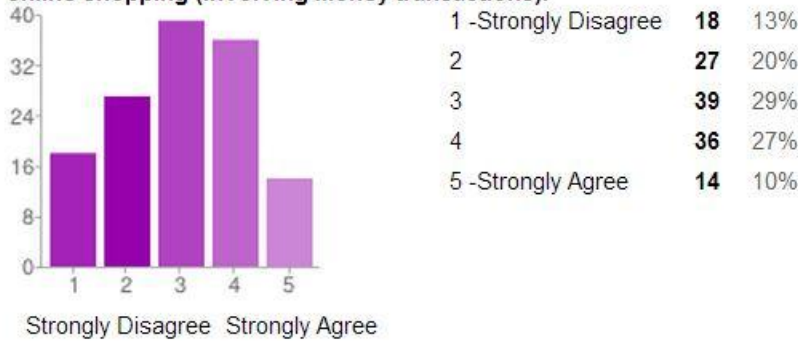


Figure 30: Biometric used for online shopping (involving money)

It’s interesting to follow the previous question with one that is much simpler, but got a much higher agreeable percentage. In figure 31 are the results of those who would prefer to use a biometric method to access their car (46%) compared to 31% for those who would not prefer this situation. Using biometric technologies for something simpler like opening the door to your car surprisingly got a positive response. This is possibly because for young adults, their car is the most expensive thing they own. It is also possible that young adults are more forgetful and lackadaisical and would love the idea of not having to carry car keys with them all the time.

I’d like to access my car using a biometric method (face scan, iris scan, or voice), so that I wouldn’t have to always carry the car key with me.

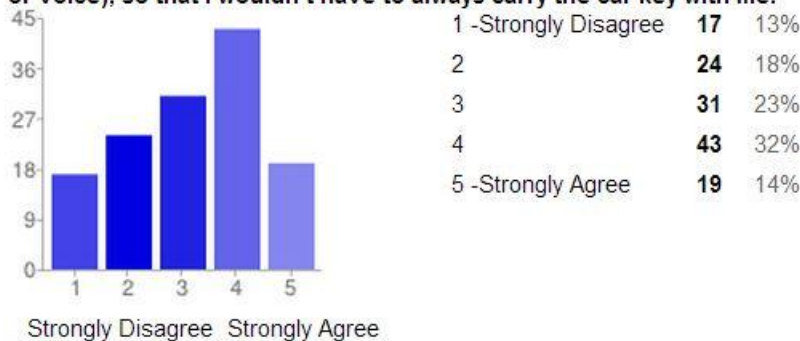


Figure 31: Biometric used to enter a car instead of keys

This is a question that showcases the age group being studied. Here a majority of the participants chose to stay neutral when answering this question (38%). In figure 32 it is shown

that 30% of respondents agreed they would prefer to use a biometric card for entering a building, an office, laboratory or parking lot, where 31% disagreed with the situation. Young adults generally don't have to enter buildings, offices or laboratories as they would if they were already in their career.

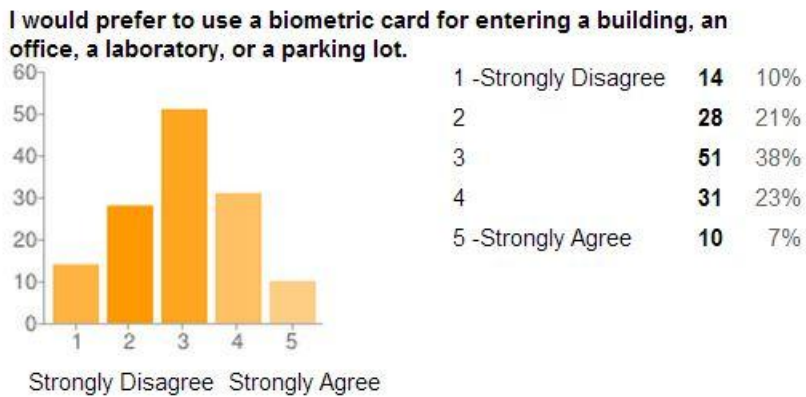


Figure 32: Biometric used for entering a building, office, laboratory, or parking lot

In figure 33 is the data of who would install a biometric system for home security. Many young adults don't yet own a home, but live on a campus or still live with their parents. Either way, 38% of respondents were agreeable that they would install a biometric system on their home. The results in this question are not heavily weighted in either direction; rather they present a normal bell shaped curve.

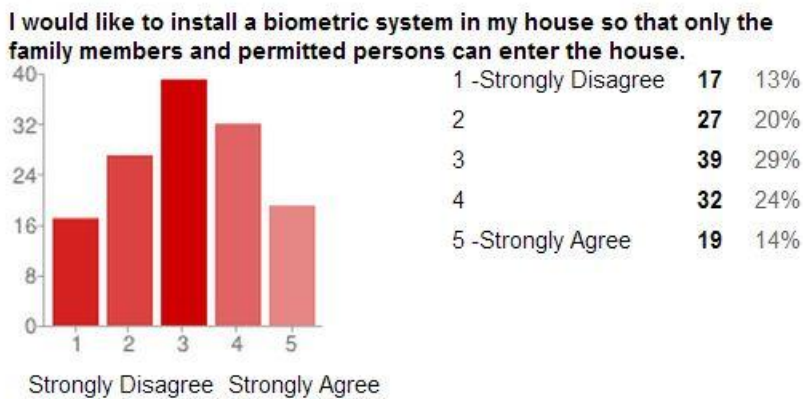


Figure 33: Biometric used for entering the home

In the personal use section of survey data there are only a couple of significant findings. Findings lineup fairly well with the age group as the participants felt strongest about logging into a computer, and entering their automobile which are generally very important elements to the young adult population. The information found here would be very beneficial to both computer and car manufacturers who target the young adult demographic as they could possibly add a fingerprint scanner and attract some additional customers.

Attitude of Providing Biometrics

Using biometric systems for your own security or for making something easier is generally a simple decision, if the costs aren't too high. It is a different story if the government or a company is going to take your biometric information to keep tabs, or run a background check. In this section the young adult's attitude toward providing their biometric information will be analyzed.

The first question in this section asks if the participants would be willing to release their biometric information to a potential employer for a background check. There was a very positive response to this question with 51% of respondents who agreed. It's important to note that 58 respondents only agreed compared to 12 respondents who strongly agreed with this question. So the participants would generally be willing to provide the information but few would provide it enthusiastically. This could possibly be attributed to the fact that the sample is 100% college students who are working hard for their future career, and they wouldn't want to lose a job opportunity because of not getting a background check.

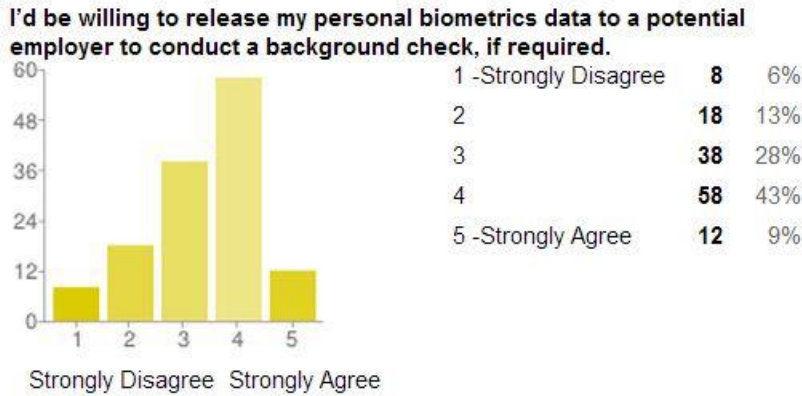


Figure 34: Willing to release biometric information to a potential employer

In Figure 35 we see even a stronger positive response to having physicians use biometric information to access medical records. There were 71% of respondents who agreed with this situation, although again the answer of “agree” received 75 answers where “strongly agree” received only 20. This is interesting because one would assume the baby boomer generation and seniors would feel this strongly toward physicians accessing their medical records, but maybe not young adults at similar levels. It may possibly be because they see the doctor as someone who knows so much personal information about them already, especially their physical body.

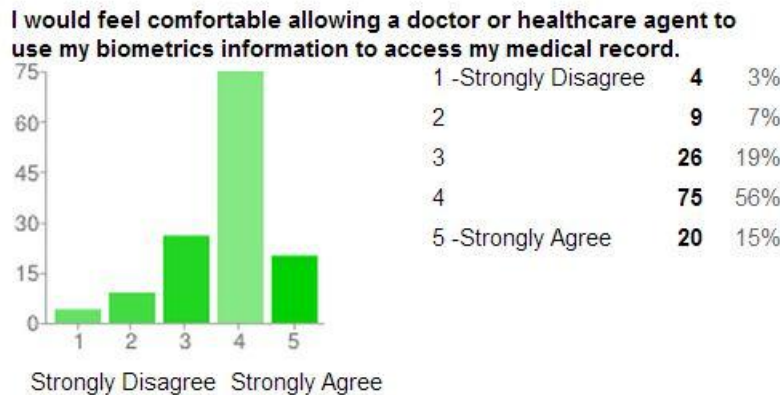


Figure 35: Willing to let doctor use biometric information to access medical record

Again, in figure 36 is the participants’ response to having their biometrics taken to obtain a passport and the response is immensely one sided. There was 75% of the participants that

agree, and only 7% that disagreed. This could be attributed to the fact that the young adult respondents may not have needed a passport at this point in their lives and therefore didn't see a downside to answering so positively. It may be that the respondents know how important a passport is to national security and so they feel very strongly about using biometrics for this purpose. It is possible that both of these ideas played a role in their decision making.

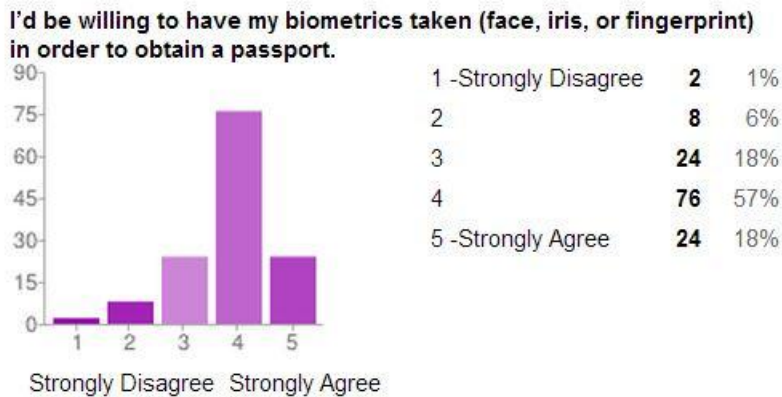


Figure 36: Willing to provide biometric information to obtain a passport

The participants were asked if they would feel comfortable having their biometric data taken in order to obtain a driver's license, and the results are in figure 37. Surprisingly, the participants answered heavily on the side of "agrees" (56%). The participants answered stronger to this question than having a biometric to enter a car instead of a key. It is possible that many of the young adults in the sample see fake IDs a lot being in college, which could influence their answers to this question.

I would feel comfortable having my biometrics data taken in order to obtain a driver's license.



Figure 37: Willing to provide biometric information to obtain a driver's license

In figure 38 is the percentage of respondents who would feel comfortable having their biometrics taken to obtain a university ID card. The results are not as strong as the last few previous questions, but 46% still answered agree or strongly agree. The participants possibly do not see the need for as much security as necessary for a passport or driver's license. These results line up with the fact that passports and driver's licenses are seen as much more trustworthy forms of identification.

I would feel comfortable to have my biometrics taken to obtain a university ID card.

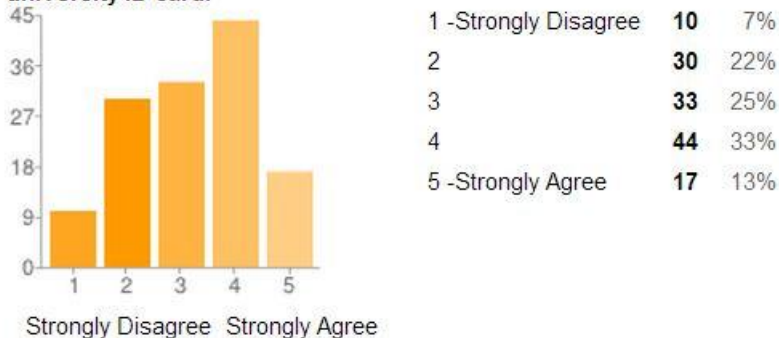


Figure 38: Willing to provide biometric data to obtain a university ID

Money is a very important part of a young college student's life. In figure 39 it is shown that 53% of participants agreed that they would be willing to have their biometric data taken to open a bank account. The participants have continuously showed a generally accepting attitude

toward the use of biometric technologies in their daily life as well as being willing to provide their biometric information. The results in this question follow suit to the answers generally given in this survey.

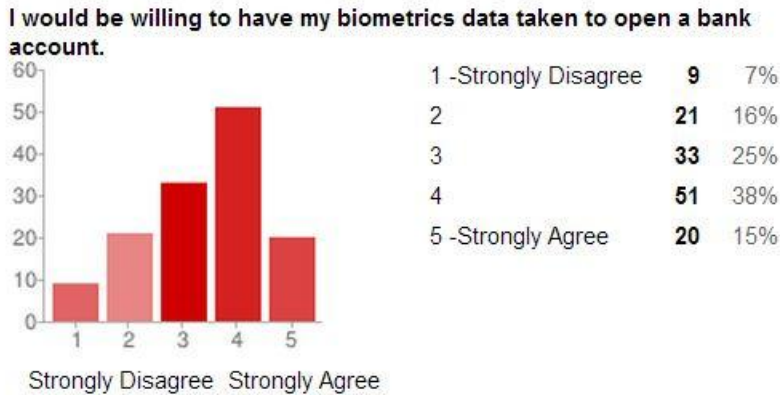


Figure 39: Willing to provide biometric information to open a bank account

The question that provided the data in figure 40 was one that could easily cause a heated debate. The participants answered with 47% who agreed they would feel comfortable letting the hospital take biometrics of all new-born babies. It's important to note that the results in this question do not conform to the normal bell curve as more people strongly disagreed (16%) than just disagreed (14%). This is a question that borders on other heated political and medical discussions such as abortion, which is where I believe the stronger disagreement response resulted from.

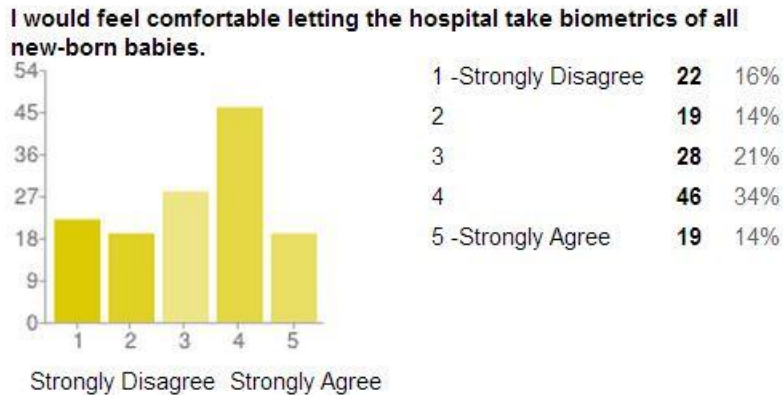


Figure 40: Comfortable with a hospital taking biometric information from new-born babies

In this section we found that the young adult population is not afraid to provide their biometric information to companies, the government or universities. The one topic that resulted in some push back is the one that involved new born babies. There will always be a stronger push back with a topic that involves infants, as they can't choose for themselves. Interestingly in this section we saw some very strong support of providing biometric information, but there is still the question of how the sample feels about entities that control the information.

About the Technology Advancement

In the sixth section the participants were asked a series of questions aimed at measuring their feelings on topics that will help the advancement of biometric technologies. I would categorize the young adult population's feelings toward biometric technologies to this point in the survey as generally favorable, but still skeptical. It is ever important that as the government and companies wish to improve future biometric systems, that they take the answers to these questions into consideration.

In figure 41 it is shown that the sample population is still generally unsure whether or not biometric technologies are more reliable and secure than traditional methods such as a password.

The majority of the participants answered neutral (40%) to this question. If you add the percentages of those who answered agree or strongly agree there were 54% of the participants. It is encouraging that only 6% disagreed or strongly disagreed, but the sample showed hesitation as such a large number of respondents answered neutral.

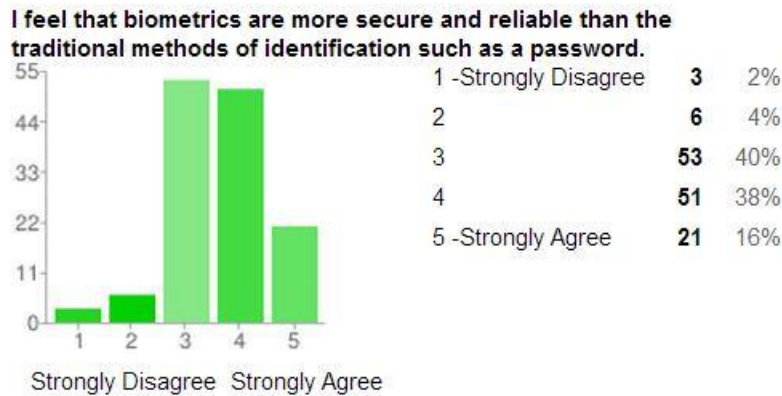


Figure 41: Biometrics are more secure than traditional methods

One of the U.S. population’s greatest concerns about all new technologies is how much time it takes to use the technology. In figure 42 is the maximum waiting time that the young adult population would wait when using a biometric method to login to a computer. The majority of the participants answered the smallest time option given, 5 seconds with 36%. There was 35% of the participants who answered 10 seconds which is probably more reasonable for biometric technology as any biometric system has to match biometric data to one instance in a very large database. Like any other technology, those who wish to incorporate biometric technologies need to make sure that they are time efficient as the public in general has a short tolerance for wait time.

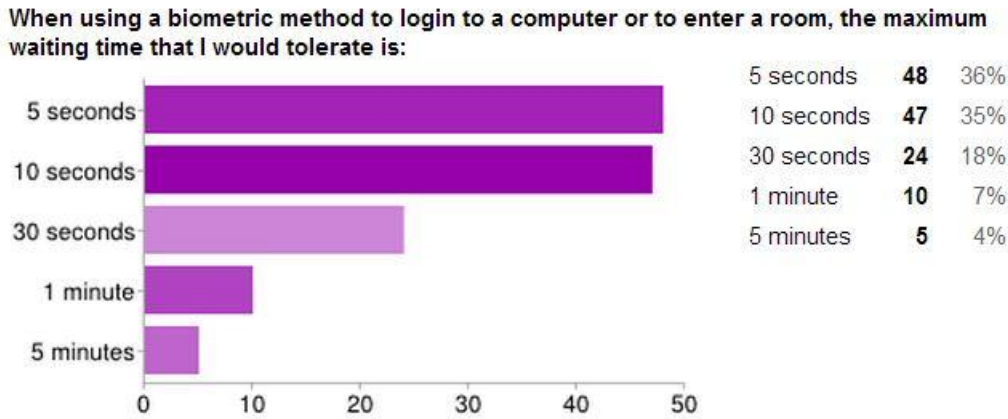


Figure 42: Maximum waiting time that would be tolerated

The results in figure 43 are not surprising. In this era, the public’s level of trust of the government is immensely low. With the portrayal of the U.S. government in the media, as well as a poor economy, talk of a financial cliff, and a continuous stalemate in Washington there is only skepticism in the general public’s mind. The young adult population is no different as 41% of participants answered neutral. The fact that “strongly disagree” received the second most responses with 19%, as well as 37% overall that disagree; there is no doubt that the government needs to heavily increase their efforts to build trust in the U.S. government if they want widespread user adoption of a biometric system.

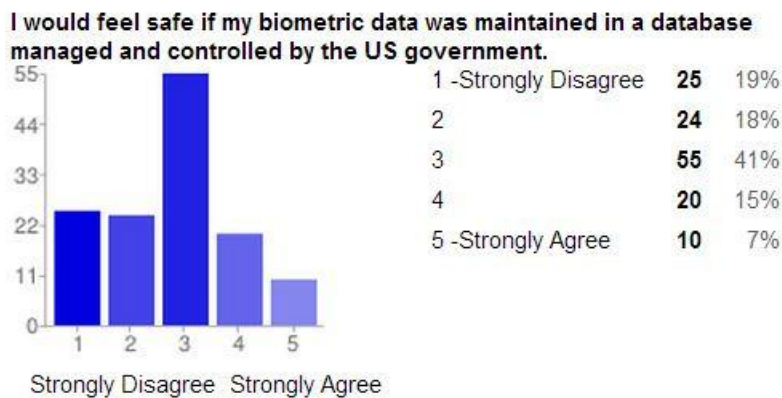


Figure 43: Feelings toward government control of biometric data

Even more interesting is the mistrust in a company or university controlling a database of biometric data. The participants answered very “neutral” again with 40%, but 44% of the participants answered “disagree” or “strongly disagree”. It is difficult to know which the participants feel less comfortable with, a company, or a university, but either way the participants do not feel safe with either controlling a database with their biometric data. This may be because the participants feel that a company or university does not have use for such private information. The government can use biometric information to catch criminals, to decrease identity theft and many other purposes, where a company or university would use this information for much more trivial reasons.

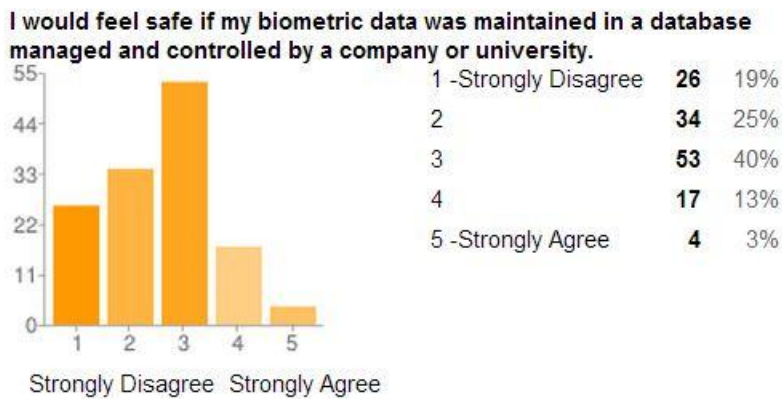


Figure 44: Feelings toward company or university control of biometric data

The results shown in figure 45 show that young adults are very favorable to increasing the amount of surveillance cameras in public areas. 58% of respondents agreed they would feel safer with more security cameras at public places. Noteworthy is that 100% percent of the respondents are college students and because of this they all have some connection to this question.

I would feel safer if there were more surveillance cameras at public places such as a college campus or a shopping mall (that may be operated without public awareness).

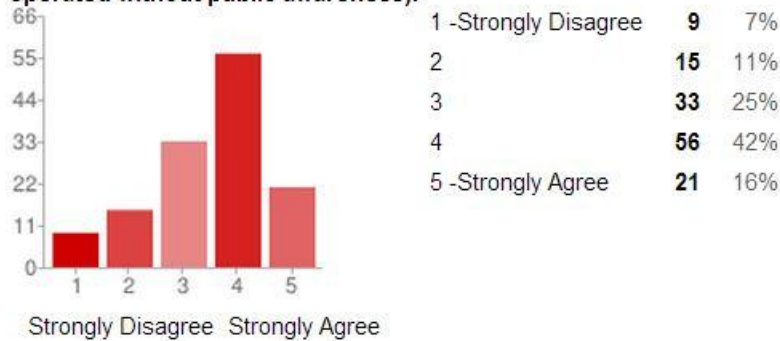


Figure 45: Feelings toward increasing surveillance cameras at public places

In this section we definitively see that even young adults are skeptical about who controls any biometric information stored in databases. They also are still unsure about the security and reliability of biometric methods. Finally, like any other technology, the amount of time it takes to use biometric information is a critical component as 71% of respondents would wait a maximum of 10 seconds. The government and companies who wish to institute biometric technologies have a lot of work to do to keep advancing the technology in the coming years.

Future of Biometrics

The future of biometrics depends heavily on the willingness of the users to adopt the technology both in the public sector as well as the personal sector. The questions asked in this section are to measure how young adults feel about where the technology is going and how they would feel in future situations.

In figure 46 are the results to the question of whether or not biometric technology is more secure than it was 5 years ago. The most important fact in the results is that only 7% of the respondents answer “disagree” or “strongly disagree.” Although 37% answered “neutral,” this is still a very positive statistic for biometric technologies. This shows that the sample believes

biometric technologies have grown in the last 5 years, which is an important step to building trust in the future of biometric technologies.

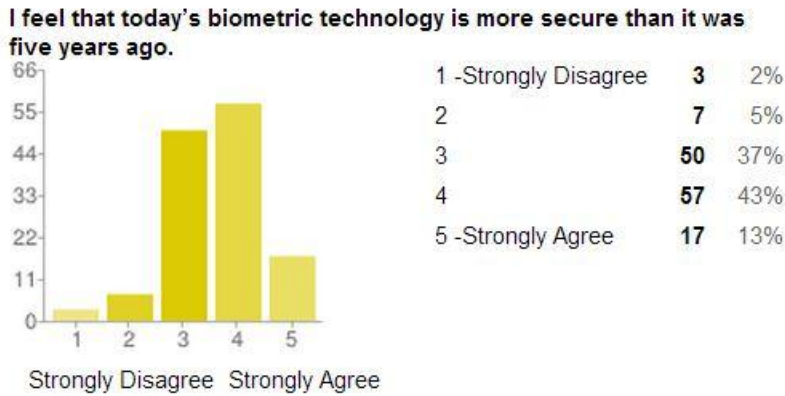


Figure 46: Biometric technology is more secure than it was five years ago

The results in figure 47 show one of the most undecided results of the survey. The participants feel neutral about whether or not government spending on biometrics research should be significantly increased with 52% of participants. This could be attributed to how many other problems we have in the United States right now, especially involving money. Both the continued recession as well as the threat of a national debt financial cliff would affect the answering of this question by the participants.

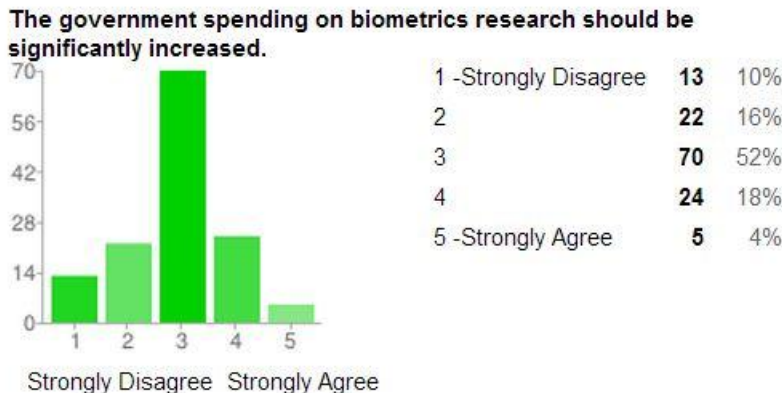


Figure 47: Government spending on biometric research should be increased

The participants are somewhat unsure whether the use of biometric technologies in our society should be largely increased with 41% who answered “neutral.” The rest of the sample marginally felt agreeable with 37% compared to 22% who disagreed. With so many other concerns in the world, even young adults see the benefits of biometric technologies but are generally unsure whether its use should be increased.

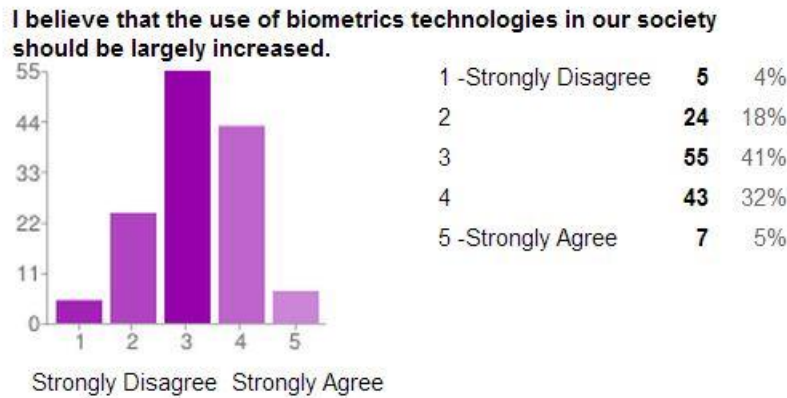


Figure 48: Use of biometric technologies in our society should be largely increased

Although the sample is generally unsure of whether or not biometric use should be largely increased, they do anticipate that the use of biometric technologies will be largely increased (58%). There is still some hesitation in the participants’ answer of this question (32%), but with only 9% who do not anticipate an increase in biometric technology use, the participants can see growth in the field of biometrics. It is encouraging to see that young adults anticipate an increase in the use of biometric technologies in our lives, this way they are more likely to adopt these technologies when their employer or the government requires their cooperation.

I anticipate that the use of biometrics technologies in our society will be largely increased.

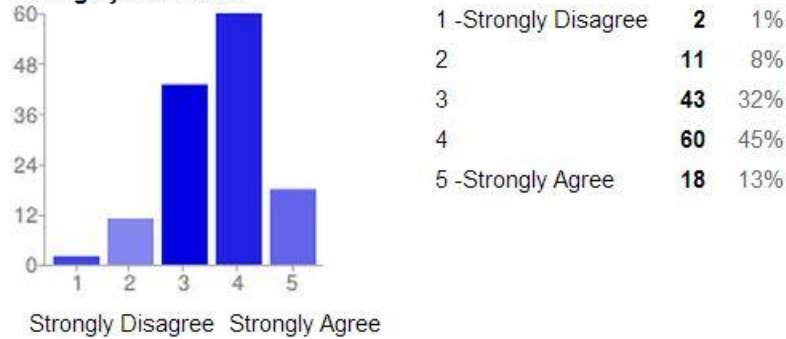


Figure 49: Anticipate the use of biometric technologies will be largely increased

The final question that we asked the participants was if they had any suggestions for the future of biometric technologies. This was not a mandatory question and most of the respondents did not answer, but you can see a list of responses from the ones that did in figure 50. I will list some of the more interesting responses. “It needs to be quick and cost efficient, if it is neither of those things, people will not accept it.” This epitomizes some of the details we have found in this survey as the median household income declined for two consecutive years from 2009-2011 [5]. Time is definitely a factor on whether or not a biometric system would be successful. “It all seems cool, but actually how reliable is it? How reliable is the technology? I feel the identification part would be safer but if the technology is a bigger inconvenience then it is convenient for the people it might be not be successful.” This is another clear point we have found from these results. The technology needs to be proven as a convenience as well as reliable for it to be successful. Both “Not use for government unless commit a federal offense. Government already has too much power”, and “Government shouldn't control it” were answered, which shows a very specific hurdle for the future of biometrics.

What new features would you recommend for the future generations of biometrics technologies?	
1	I feel that biometric technology is an amazing technology that is helping to advance both America and the rest of the world, but it would HAVE to be completely secure with no glitches in order to gain my full trust.
2	Finger print scan for login and personal identity topics wether personal or in public.
3	Iris recognition for all transactions would be beneficial. Companies could scan and make transactions instead of bill transaction. It could save a lot with paying at a store.
4	It could be used to avoid people cheating on exams, such as the ACT. If they are required to give biometric information rather than just a photo ID. The average student would probably not have the ability to get past that technology. Where a photo ID could be fake or they may look similar to their sibling or friend.
5	Instead of a number or word password use a touch tone password. Have a keyboard instead of the blank box to type in the password and touch they keys to create a personalized tone that becomes your password.
6	I think they should have more than just one biometric feature such as a finger scan and and eye scan.
7	-Keyless car entry -Biometrics for cell phone purchase, online shopping, creating new accounts online, applying for credit cards, houses, or a new car -My idenity was stollen by an ex boyfriend, that memorize my Social Security number, biometrics would be an amazing idea to prevent this from happening again
8	Just to be careful. If they are going to use for unlocking cars, it should not take more than 5 seconds. Just in case if someone was running from someone dangerous.
9	It has to be quick and cost efficient. If it is neither of those things, people will not accept it.
10	I liked the idea of using it in your home to only allow certain people in and gunstores using it to check people looking to buy a gun.
11	Along with identification, these biometric technologies could also keep logs of your movements and activities. Thus keeping a detailed record that could be accessed only when needed.
12	It all seems cool, but actually how reliable is it? How reliable is the technology? I feel the identification part would be safer but if the technology is a bigger inconvenience then it is convenient for the people it might be not be successful
13	For biometrics technologies to work in the future, better cameras would have to be designed. There are many people who look alike, talk similar, and walk the same way. Also, setting up fingerprint, eye, facial, or any other readers would be a very time consuming and costly to all technology already in use.
14	I use biometrics for my part time job. It takes my fingerprint. The problem is, it does not always take all the time. It takes a lot of tries. I think having the option of putting a password in, would also be beneficial.
15	I like the idea for public schools to use biometrics but not so with college campuses. Colleges are large and I think it would create more of headache to keep track of all the students on campus. In conclusion I feel that someone may want to take a look at the question "At a college or high school, the administration could use a biometric method to screen people entering the campus for security reasons." I put a 4 for this question only because it mentions high school, not colleges. Thank you and hopefully you take my feedback into consideration.
16	I can't think of anything right now, but maybe something with cameras or something.
17	None, the world is fine the way it is.
18	I have nothing I can recommend because I know very little about biometric technologies.
19	I can't think of any new technologies at the time that haven't already been invented. I like all the ideas of biometrics technology for the advancement of our society.
20	Hand/face scanners to open doors or login to certain websites
21	Not use for government unless commit a federal offense. Government already has too much power
22	Retinal Scans for everything. Can't change retinas very easily.
23	Biometrics for all personal records and accounts, credit cards, debit cards, and bank accounts
24	Making sure that if a persons DNA is taken that it can not be used
25	None I don't know enough about it.
26	for them to be more sensitive to the things they scan there or crazy smart people out in the world that can get around them and steal your identity. I would say if you use biometrics you still have to use an I.D.
27	None, I think that more technology with biometrics is really unnecessary in some cases
28	I don't recommend biometrics at all. I don't feel that it will be of any use.
29	To just make them more affordable really. To also make sure they cannot release a person's genetic identity.
30	None that I am aware of.
31	Government shouldn't control it.
32	I'm not sure because I know very little about biometrics
33	Eye retina checks
34	None, thank you.
35	Specific Sound Patterns
36	To require more than one at a specific time password/and biometrics for double security
37	Fraud Detection
38	Eye scan (laser scan)
39	I think that they should use hair to identify people
40	Just focus mainly on security with official buildings, universities, etc.
41	More convenience. At this point, for recreational use biometrics are still less convenient than inputting a password
42	Fingerprint scan to access bank account. Some type of scanner or render to enter your vehicle
43	It's the future but until it is safe enough and all data cannot be stolen, enforced or replicated. It is to risky.
44	I cannot come up with any.

	Use more than one at a time (i.e. face and fingerprint)
45	Full body biometrics
46	I wouldn't recommend any, I'm not a strong believer in it and I think it's an inconvenience and too personal.
47	An identification card issued by the government that holds all of your biometric information. This would allow biometric checks to be done against the id card instead of multiple organizations/businesses having a database containing my biometric information. This would allow for faster checks and would keep my information more secure.
48	none, I don't feel safe, as of right now, with this kind of technology.
49	I don't really mind the biometric technologies and I don't think it invades privacy but I guess my recommendations would be to keep working on it because I like to feel safe in my country.
50	Making an army of my clones.
51	The optional use of biometrics for use of access to devices such as smartphones, iPods, etc. and for access of allowed personnel for extremely important information in relation to the government. Also, banks should use biometric systems.
52	don't take advantage of the info
53	Start slow such as vehicles.
54	Using it to clock in for work, and using it to cash a check
55	When signing your signature for using a credit card, you should use your finger print instead of signature.
56	biometrics for safes at cheaper prices.
57	I believe that the most fast and efficient biometrics are already in existence.
58	maybe taking your fingerprint when you try to withdraw large amounts of money
59	That before biometric technology can be used worldwide it needs to be greatly improved. Maybe a hair sample could be used, they could do a scan of your hair and face to recognize you.

Figure 50: What new features would you recommend for the future generations of biometrics technologies?

The future of biometrics is promising but will not be successful unless certain aspects are truly taken into consideration. Young adults are believed to be the most willing to adopt technology, but if there is sufficient hesitation from young adults toward the use and trust of biometric technologies it can be assumed that the baby boomer generation and seniors would be even more skeptical. The government and any corporate entities that wish to implement biometric systems should heavily consider the data presented in these results.

Conclusions of Survey Findings

The survey has measured many aspects of how young adults feel about biometric technologies. Some of the most important details that were found include the mistrust of the government, the uncertainty of the entities that would control the databases of biometric information, and the general favorable attitude toward the use of biometric technologies. These are very important details for the present and future use of biometric technologies.

The major findings of the survey study are:

- **Basic Knowledge of Biometrics** - It can be concluded from the results in this section that young adults need more education and experience to build trust in biometric

technologies. When introduced to the biometric methods, they are familiar with the use of fingerprinting for identification purposes but are generally unaware of any others. The results are encouraging as the participants trust that biometric data is unique (reliable), but they are unsure whether or not the data can be duplicated (secure).

- **Concerns of Using Biometric Technologies** - We conclude that young adults have concerns and benefits that align with their own personal concern before anything else, especially the topic of identity theft. The benefit that biometric technologies can provide great ease and convenience can get overlooked. There are many people that still view biometric technologies as an inconvenience and hassle and these views need to be changed if biometric technologies are going to be increasingly successful in the coming years.
- **Acceptance of Biometrics Used by the Government and Organizations** - In this section we gained some very distinct feelings of the young adult population toward biometric technologies. Some of these feelings could even be applied to the population as a whole as the situations are not specific to age. Generally the young adult population showed in this section that hassle is a concern, they are concerned with the safety of their money, and they are generally accepting of biometric use.
- **Acceptance of Personal Use of Biometrics** - In the personal use section of survey data there are only a couple of significant findings. Findings lineup fairly well with the age group as the participants felt strongest about logging into a computer, and entering their automobile which are generally very important elements to the young adult population. The information found here would be very beneficial to both computer and car

manufacturers who target the young adult demographic as they could possibly add a fingerprint scanner and attract some additional customers.

- **Attitude of Providing Biometrics** - In this section we found that the young adult population is not afraid to provide their biometric information to companies, the government or universities. The one topic that resulted in some push back is the one that involved new born babies. There will always be a stronger push back with a topic that involves infants, as they can't choose for themselves. Interestingly in this section we saw some very strong support of providing biometric information, but there is still the question of how the sample feels about entities that control the information.
- **About the Technology Advancement** - In this section we definitively see that even young adults are skeptical about who controls any biometric information stored in databases. They also are still unsure about the security and reliability of biometric methods. Finally, like any other technology, the amount of time it takes to use biometric information is a critical component as 71% of respondents would wait a maximum of 10 seconds. The government and companies who wish to institute biometric technologies have a lot of work to do to keep advancing the technology in the coming years.
- **Future of Biometrics** - The future of biometrics is promising but will not be successful unless certain aspects are truly taken into consideration. Young adults are believed to be the most willing to adopt technology, but if there is sufficient hesitation from young adults toward the use and trust of biometric technologies it can be assumed that the baby boomer generation and seniors would be even more skeptical. The government and any corporate entities that wish to implement biometric systems should heavily consider the data presented in these results.

If the government wishes to implement a nationwide biometric system then the public must be won over. Trust will have to be earned. Convenience, security and reliability will have to be assured to the public. These steps are all imminent and justified as the public deserves to have their trust rewarded.

References

- [1] Lease, David R. "Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information Technology and Security Managers." Diss. Capella University. October 2005. P. 143 Print.
- [2] Duane Blackburn, Chris Miles, Brad Wing, et al. *Biometrics Frequently Asked Questions*, 2006. Print.
- [3] McLaren S, "Reliability of Iris Recognition as a means of identity verification and future impact on transportation worker identification credential," 2008. P.33 Print
- [4] Ashbourn J, "The Social Implications of the Wide Scale Implementation of Biometric Related Technologies." Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, 2005. p.4 Print.
- [5] U.S. Department of Commerce. Census Bureau. *Income, Poverty, and Health Insurance Coverage in the United States: 2011*. September 2012. p. 1 Print.
- [6] U.S. Department of Commerce. Census Bureau. *Age and Sex Composition: 2010*. May 2011. P. 4 Print.
- [7] Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. 1989.
- [8] Opinion Research Corporation International, "Public Attitudes Toward the Uses of Biometric Technologies." SEARCH.ORG, p. 46 Aug 2002.
- [9] Rubas, Debra, "Technology Adoption: Who is Likely to Adopt and How Does the Timing Affect the Benefits?" Diss. 2004. p.50-51. Print.

October 29, 2012

Dr. Yong Zhang, Principal Investigator
Dr. Julie Blaskewicz Boron, Principal Investigator
Mr. Anthony Allen, Co-investigator
Mr. Ross Morrone, Co-investigator
Department of Computer Science & Information Systems
UNIVERSITY

RE: HSRC Protocol Number: 030-2013
Title: A Quantitative Study of the Social Impact of Biometrics Technology

Dear Drs. Zhang and Boron and Mr. Allen and Morrone:

The Institutional Review Board has reviewed the abovementioned protocol and determined that it is exempt from full committee review based on a DHHS Category 3 exemption.

Any changes in your research activity should be promptly reported to the Institutional Review Board and may not be initiated without IRB approval except where necessary to eliminate hazard to human subjects. Any unanticipated problems involving risks to subjects should also be promptly reported to the IRB.

The IRB would like to extend its best wishes to you in the conduct of this study.

Sincerely,

Peter J. Kasvinsky
Dean, School of Graduate Studies and Research
Research Compliance Officer

PJK/cc

cc: Dr. Kriss Schueller, Chair
Department of Computer Science & Information Systems