Social Acceptance of RFID as a Biometric Security Method

Christine Perakslis and Robert Wolk
Bridgewater State College
Cperakslis@bridgew.edu, rwolk@bridgew.edu

Abstract

The acceptance of biometric security controls in documentation, travel, and employment may soon be facing a strong test as it is further expanded through RFID, with advocates of global security aggressively working toward broadening the scope of tracking to the individual human level through implanted chips. Implanting chips in humans has only recently come to the forefront, as the FDA approved implantable RFID chips for medical purposes in October 2004. Yet national and international polls show that consumer awareness is low relative to biometric methods as well as RFID technology. Though study results substantiate that the general population is acutely concerned about privacy and personal rights protection, data reveals that consumers place a heightened value on convenience. These factors, coupled with the looming threats such as terrorism and identity theft may create the "perfect storm" in which consumers forgo the battle to ensure control over when and by whom they can be perceived by others.

1. Introduction

The events of 9-11, the growth of globalization, and the converging interests of the information age have all combined with a sense of urgency to develop new sciences such as biometrics and RFID (Radio Frequency Identification). Following past success with other emerging technologies, the academic, government, and industry components of a technology-based culture have all combined their efforts in a way that has had results in the past. Creating standards has worked for other new technologies from the personal computer to the Internet. Elements of a standards network of organizations were already in place. Driving this development of new standards were eminent threats to the dominant social order of an expanding and increasingly vulnerable world culture based on technology and the sharing of information. A culture relying on ever more complex systems needed a way to quickly ensure the safety of that system and those that relied upon it.

Biometric methods offer more secure and convenient processes compared to alternative methods of identification. In contrast to a hand-carried object or a pin access code that can be stolen or forgotten, biometric methods identify the unique aspects of the user's physical being. The pattern-recognition system identifies a person based on a feature vector derived from specific physiological or behavioral characteristics.

The integration of technology such as RFID with biometric methods enhances the accuracy and security of biometric identification, and also provides easily accessible data on an RFID-enabled object that can be accessed by a reader. Biometric characteristics can oftentimes be obtained through covert recognition, without an individual being aware. Thus, in the case of a passport verification process using these technologies, the identity management system not only verifies the person's identity by a physiological characteristic match through the biometrics, but also can access and authenticate against an RFID chip housing key data unique to that individual such as a identification code, pin code, name, date of birth, date of departure, country of origin, and possible alternative biometric secondary data such as an iris scan for backup identification as necessary.

If the combined use of these technologies were then fused together with multiple databases subsequently linked to one national database, this centrally controlled information bank would be then be expediently accessible for identification and tracking of each citizen. With these emerging technologies, government, healthcare, academic, and industry components of our culture are likely to combine their efforts to collect and share pertinent information on a real-time basis.

Yet objects such as passports can be stolen or misplaced. Therefore, an anticipated solution is to implant a small means of identification within humans that would hold a unique identification number and possibly other pertinent information such as pre-existing medical conditions or emergency contact information. When a reader activates this small implanted device, authorized agents would be able to unlock pertinent information from the centralized database.

Proponents of this emerging technology argue under the aegis of personal and national security, enhanced working standards, reduced medical risks, protection of personal assets, and overall ease-of-living. Corporations such as Applied Digital Solutions and Digital Angel have already developed chipping methods. From Stockholm, Sweden to Sutter, California, primary schools are now implementing tracking and authentication methods for

0-7803-9284-1/05/$20.00 ©2005 IEEE

children utilizing biometrics and RFID. Primary school students in Osaka, Japan are now being chipped with RFID.

Although there is societal acceptance of fingerprinting, retinal scans, face recognition, and voice recognition, acquiescence to the implantation of a chip into the human body may prove a far more significant challenge. Though the present world realities warrant greater security measures, global standards must encompass information protocols and protections to guarantee that the use of a global information system would truly serve those that rely upon it for protection at not only a national level, but also an individual level.

Instinctively, the foreboding questions explode as to who controls this massive warehouse of information and with what intent now - and with what intent far into the future. The concept of the ubiquitous tracking of humans has undoubtedly caused much controversy relative to policy and privacy issues. Though advocates for tracking pervade many components of our culture, they are often those who stand to gain advantageous control through individual-level tracking. Though there are great benefits with these technologies such as expedited services, enhanced border controls, anti-terrorism systems, and the much-coveted conveniences, information is a powerful tool that must be utilized responsibly and within the confines of stringent accountability.

2. Biometrics & RFID: Social Awareness

When reviewing the societal acceptance of biometric technologies, exclusive of implanting unnatural unique identifiers into the human body, acceptance seems to be increasing steadily and appears to be driven by three major forces: terrorism, identity fraud, and convenience. Though there is a balancing drive in society to ensure that identification methods provide individual privacy, security and safety, recent surveys show that individuals want the methods to be just as convenient as they are secure. Yet, it is imperative to note that data illustrates that within the general populace, awareness is low relative to biometrics as well as RFID.

In addition to an anemic understanding, misunderstanding exists for those respondents aware of the technologies and the sources from which the populace is gleaning their information on these technologies are atypical.

2.1 Societal Awareness is Low, but Increasing

Cap Gemini Ernst & Young surveyed samples representative of the population in the U.S. in 2003 and in Europe in 2004 to measure consumer perception of RFID technology in uses such as retail and expedited services (non-inclusive of methods integrating biometrics). The study shows that although favorable responses to the consumer's perception of RFID were 42% and 52% respectively, the combined responses of "No Opinion" and "Don't Know" relative to the perception of RFID technology were 48% for the U.S. and 40% in Europe, indicating a deficiency in consumer awareness. Parallel to this, consumer understanding of the technology itself is insufficient. Interestingly, more than 75% of respondents indicated that they had used or were aware of services using RFID technology, yet the respondents did not recognize RFID as the technology utilized in these processes [18].

For those European consumers who are aware of the technology, the survey indicates that their information was attained primarily through printed media (37%), the Internet (29%), television (16%), and word of mouth (12%). According to Cap Gemini's data, Americans surveyed had learned of RFID predominantly by word-of-mouth rather than traditional methods such as mass media [18]. According to an alternative study done by BIGresearch and Artafact LLC, Americans learned of RFID predominantly by educating themselves by means of the Internet [3].

When reviewing the study commissioned by SEARCH, the National Consortium for Justice Information and Statistics, relative to the awareness of biometrics, data reveals that although personal experience with biometrics has increased slightly (from 3% in 2001 to 5%, representing 10 million people, in 2002) merely half of the general public was aware of the technology [17].

Yet awareness is beginning to increase more rapidly, as biometric methods are being utilized more frequently and combined with technology such as RFID. In a more recent study done by BIGresearch and Artafact LLC, data reveals that awareness of applications utilizing technology such as RFID had increased from 28% to 35.5% just in the last quarter of 2004 [3]. More frequently, headlines are also highlighting advances, benefits, and intended uses in the fusing of these technologies.

According to a survey on the perception of biometrics, individuals introduced to the concept of biometrics tend to initially have a positive attitude toward its use. Yet, when considering the increased use of biometric technology in their private lives, individuals become more skeptical. Individuals have many apprehensions when considering the use of biometrics and the general feeling is one of being potentially exposed through a system that has not yet been systematized as it relates to security and reliability. Social factors relate to perceptions, which will play a key role in the further acceptance of biometrics as is also likely when considering the uses when fusing these technologies [7]. As Ilse Geilsing further describes:

"Social factors are aspects that describe intrinsic human values that cannot be changed fundamentally in any way and relate to human behavior that links with human perceptions and attitudes. There are always factors, which could be of a technological nature or of a social nature, that obstruct emerging technology adoption. In the case of biometrics, these include user perceptions related to biometrics, the potential loss of privacy, false acceptance rates, device deployment difficulties… trust is important in the adoption of new technologies such as biometrics [7]."

2.2 Increases in Everyday Uses

The UK Government will start introducing national identity cards on a phased basis as soon as August 2007, with plans to have 80% of the economically active population covered within five years. Britain will utilize biometric data linked to a national database that will provide a secure means to impale identity fraud, immigration abuse, illegal working and organized crime. By mid-2005, biometric passports are planned for issuance incorporating an RFID chip holding facial biometrics, with a subsequent possible launch that will include iris and finger recognition.

In the U.S., a recent vote in the House of Representatives approved a measure by the name of the Real-ID Act that would require states to generate standardized and electronically readable driver's licenses by 2008 in compliance with federal antiterrorist standards. The features of this ID card will include anti-counterfeiting elements, machine-readable technology with defined minimum data elements, and a digital photograph. Due to the voluntary nature of obtaining a driver's license, the U.S. government asserts that this is not a National ID. Yet without this "smart" license, a U.S. citizen is likely to be refused access to trains, airplanes, national parks, courthouses and other federal buildings. The bill also establishes that states will be required to link all DMV databases if they desire to receive federal funds. The technologies being considered include biometric information such as retinal scans, fingerprints, DNA data and RFID tracking technology [10].

Retail desires transparency throughout the supply chain by tagging individual items with RFID-enabled tiny chips. Yet with this technology, there exists a new power for real-time market research through surveillance of shopping behaviors within the store.

Schools are taking advantage of biometrics and RFID technology, as they are cognizant of the increasingly more complex responsibility of keeping children accounted for and safe from arrival through after school programs to transport home, managing the whole lot from truancy, maintaining multiple student computer passwords, and the threats of abduction, to name a few.

Employers are exploring the advantages of utilizing these technologies to ensure only those employees authorized can enter buildings, turn on lights, access computers, change office thermostat settings and operate specialized machinery safely and according to set standards based on a system that can authenticate those employees who meet the predetermined levels of permission.

3. Obstacles: Standards

Over the past two years, there have been rapid advances in biometric standards due to US and Canadian governments, international standards bodies such as the International Standards Organization (ISO), International Electrotechnical Commission (IEC), International Civil Aviation Authority (ICAO), and International Labor Organization (ILO), which falls under the UN; as well as US and other national standards bodies such as ANSI and NIST; and industry associations such as the BioAPI Consortium, OASIS and AAMVA.

Relative to RFID, EPCglobal is leading the development of industry-driven standards for the Electronic Product Code™ (EPC), yet is also working in cooperation with the International Standards Organization (ISO). EPCglobal is comprised of eminent firms and industries focused on creating global standards for RFID. As a joint venture between EAN International and the Uniform Code Council (UCC), EPCglobal is a not-for-profit organization entrusted by industry to establish and support the Electronic Product Code (EPC) Network as the global standard for immediate, automatic, and accurate identification of any item in the supply chain of any company, in any industry, anywhere in the world. EPCglobal's primary objective is to drive global adoption of the EPCglobal Network, which was developed by the Auto-ID Center, an academic research project headquartered at the Massachusetts Institute of Technology (M.I.T.) with labs at five leading research universities around the globe. The EPCglobal Network will utilize industry best practices to protect data, while coexisting with standards set by the ISO, which is the most important standards body relative to the standardization of generic biometric technologies effecting human beings and relative to supporting interoperability and data interchange among applications and systems [6].

Despite privacy concerns and the still emerging standardization of globally-acceptable methods and means, there is an every pressing push from industry and international governing bodies to move toward identity management methods with the use of contactless, easily accessible and ubiquitous tracking systems that integrate biometric data.

These developments are currently progressing, to some extent, in a vacuum relative to public policy and

regulations. Like a frog in boiling water, our temperatures raise parallel to an environment in which there seems to be a drive to produce at the most convenient and productive pace, while all the time there may be a slow erosion of concern for the protection of personal privacy.

4. Societal Perception: Convenience, Security, Fighting Terrorism, and Reducing Identity Theft

Convenience and security are perceived advantages of biometrics and RFID use, as individuals experience the benefits more frequently in everyday usages. Fighting terrorism and reducing identity theft are also motivational drivers that may be creating a greater impetus for greater acceptance of RFID and biometrics identification methods.

4.1 Perceived Advantages: Convenience & Security

Convenience is a prevailing theme in the results of a survey commissioned by EDS and the International Association of Privacy Professionals (IAPP) and conducted by the Ponemon Institute in 2004. The study revealed that 61% of consumers do not want to be forced to change passwords as is often mandated to enhance security and 66% of consumers believe it is worse to endure the inconvenience of being denied access due to a systems glitch than it is to be given access without proving their identity.

In measuring consumer receptiveness toward methods such as biometrics and a single secure and private identification credential, the results also suggest that a majority of consumers are open to alternative identification methods such as biometrics. Data shows that 69 percent are open to the idea of using biometrics for an identity management. Relative to convenience, 88 percent of those respondents open to the idea of using biometrics are in favor of the technology for the reason that it is convenient and does not require them to remember passwords [11].

During a survey conducted on behalf of New Jersey Institute of Technology (NJIT) by Global Strategy Group, Inc. in 2002, respondents were asked about the advantages of a national identification (NID) card such as one that might contain biometric data as well as an RFID tracking device. Convenience was the second most frequently mentioned potential advantage, relative to requiring only one document for all identification purposes. The primary and tertiary perceived advantages also coincided with other national survey data and were revealed as terrorism and identity fraud , respectively [9].

Recent developments in security policy have presented individuals with an interesting bargain to exchange a measure of privacy to save time in identification methods. The United States Transportation Security Administration (TSA) is making an offer to travelers to make just that deal. To qualify for bypassing normal security checkpoints at airports the traveler, who must be a U.S. citizen or a permanent resident and a frequent flyer, can complete an enrollment form along with verified identification. The TSA will then take an approximate five minutes to collect the traveler's iris scans and fingerprint scans for the database. Once passing a background check and approved, the traveler can bypass the normal security lines once spending approximately five seconds at a machine that identifies the iris and fingerprint of the individual. The trial program ran in October of 2004 (K. Murphy, 2004). This program in effect will separate travelers into two groups: those that submit to privacy intrusions and those that will not, or do not, qualify [12].

Recently, theme parks, such as Wannado City, utilize RFID for the safety and security of families. The park issues RFID wristbands to all visitors as part of general admission, with touch screen kiosks located throughout the 140,000 square foot facility. This system makes it possible for family members to pinpoint one another's locations real-time [8].

The Ohio Department of Rehabilitation and Correction (ODRH) is planning to tag inmates in thirty-three separate facilities with RFID-enabled devices, detecting even if prisoners attempt to remove the device. Staff will also wear devices on their belts pinpointing their location real-time, for security reasons [2].

Taking into consideration national security, there is a drive in the government for the use of RFID for more comprehensive tracking. Under the sponsorship of Homeland Security the U.S. State Department will issue passports with embedded RFID chips housing all pertinent information, which are said to not only frustrate illegal immigrants and thwart terrorists, but also to expedite processes.

There has been increased focus on the uses of RFID in the retail sector, with the facts and figures verifying reduced costs, improved services, and enhanced convenience. Relative to the use of RFID technology in the retail sector, the study done by Cap, Gemini highlighted that security is considered by consumers to be the most important benefit from RFID such as improved security of prescription drugs, faster recovery of stolen goods such as automobiles, and improved food and drug safety and quality. Many respondents in Cap Gemini's study stated that they would be willing to buy and RFID-enabled product to obtain the benefits that they value [18]. This convergence of demands for security with convenience command that the consumer receive faster checkout, anti-counterfeiting assurances, reduced identity theft, improved product safety (such as recalls), in-aisle

companion product suggestions, instant recognition of preferences, reduced out-of-stocks, and decreased costs due to reductions in theft. Security and convenience are veritable drivers of the use of these technologies. Yet as the demands of the consumer are met, the merchants derive an ever-increasing powerbase while simultaneously obtaining a plethora of consumer information. The intent of use becomes the question.

Companies are embracing the use of these technologies to exploit their target markets by not only further extending the service and the convenience found in the daily use of RFID-enabled processes, but also by tracking consumer purchases and statistically determining consumer habits and drivers. The detail, frequency, locations, and product combinations of every consumer purchase can be computed, analyzed and measured. Companies such as Harrah's and Mohegan Sun have been able to define the gambling habits and distinct motivational forces of their patrons through information collected through customer reward cards.

Visa, MasterCard, and American Express are planning to simplify payment processes and provide customers with a "contactless" credit card system when making purchases by utilizing RFID. In the new system, consumers wave a credit or debit card within a few inches of a reader to complete a purchase, with no signature requirements for purchases less than $25.00. With data security issues at the forefront, Visa has publicized a well-designed and highly secured system that is alleged to have multiple layers of encryption and fraud detection. Unique codes will be utilized during transmissions; codes cannot be reused even if intercepted. The new unobtrusive process is said to afford the consumer with the much-coveted convenience and expedited service - securely.

4. 2 Drivers: Fighting Terrorism & Reducing Identity Theft

The third most frequently mentioned advantage of an NID in the study commissioned by the NJIT was for the reduction in identity theft; the most frequently mentioned advantage of an NID was a tool designed for decreasing terrorism [9].

In unison with the aforementioned study commissioned by NJIT, a public opinion poll commissioned by SEARCH determined that support for the use of biometrics in government and the private sector was yet again most strongly driven by two factors: fighting terrorism and identity fraud. This survey was recognized as one of the first representational national surveys on biometrics. Conducted in two waves (September 2001 - post 9-11, and August 2002), the survey revealed that for those aware of biometrics, public support was high at 86% in 2001 and 80% in 2002 for the use of biometrics by law enforcement for antiterrorist or crime prevention [17].

Of the survey respondents, 95% regarded identify theft as a serious problem, with 21% (or 42 million people) describing themselves as recent victims of identify theft. With the ever-increasing avalanches of data security breaches such as the misplaced backup tapes housing 1.2 million records on U.S. federal employees, a leak of tens of thousands of consumer records, erroneous access protocols leading to exposed payroll information, and even unexplained access by hackers into cell phone data, data security is an escalating issue. More than 27 million Americans were victims of identity theft over the last five years, costing consumers approximately $5 billion in out-of-pocket expenses. Consequently, increased awareness of the dire realities and dangers of data misuse is creating the impetus for the public to cry out for enhanced protection and accountability of data relating to the consumer.

The NJIT survey data also revealed that the majority of respondents (77% to 88%) supported the use of biometric technology with regard to accessing government buildings, obtaining a driver's license, verifying passport information, or checking in at airport [9]. Respondents supported private-sector use of biometrics such for services such as credit card, ATMs and paychecks.

5. Inhibitors: Privacy & Data Security

Americans value the protection of their personal information and there is high public insistence that privacy safeguards be established and maintained. Identity management issues are of becoming of paramount importance, with greater concern likely, as breaches in security are more frequently being reported.

5.1 Primary Concern: Privacy

Across the national and international surveys reviewed, as well as the sample survey performed, the authors found privacy to be the chief concern in all nations for the usages of RFID, Biometrics, and the fused usages of Biometrics with RFID (including implantable chips).

The study relative to consumer perception of RFID usages in the retail sector done by Cap Gemini Ernst & Young in 2003 highlighted that privacy concerns are the most significant issue among consumers in all countries. For those consumers who said they were concerned with RFID technology, the greatest apprehension related to privacy concerns such as consumer data being used by

third party, being targeted with more direct marketing, and being tracked via product purchases [18].

The NJIT survey in 2002 noted privacy as the primary area of concern such as governmental abuse and the access and misuse of information by criminals or unauthorized persons relative to the use of a National ID Card utilizing biometrics and RFID [9].

In the 2004 survey done by BIGresearch and Artafact LLC relative to RFID, at least two-thirds of consumers who are aware of RFID reported feeling concerned about issues with the invasion of privacy, the potential for privacy abuse, or that that companies might use the information to monitor transactions or purchasing habits [3].

With these technologies, those authorized within the system will have the capability of not only collecting, but also of storing and accessing comprehensive and increasingly detailed private information on each individual. Data would certainly be utilized for enhanced services, intelligence, and global security, but also potentially for tracking and the analysis of the patterns and behaviors of the individual. In addition, large-scale data as such would allow for a myriad of other potent areas of scrutiny such as grouping individuals to mine data based on demographic determinants or ethnicity.

Although detailed information is often collected and utilized for the enrichment of customer relationship (such as customer reward cards), there appears to be a fine line separating the altruistic motives from the methods and modes of manipulating the individual. Today, software affords the ability to statistically calculate and define techniques to powerfully influence behaviors. As processes are put in place, these advances in technology continue to transform the relationship between the individual and his or her world. No longer is the individual able to determine to whom and when they are furnishing personal information. Nor does the individual truly know the long-term intent with which this information is be used now – or well into the future. The agency or corporation that obtains your information today is likely to under another name or altered management tomorrow.

As noted in the U.S. Privacy Protection Study Commission in 1997, "the real danger is the gradual erosion of individual liberties, through the automation, integration, and interconnection of many small, separate record keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable." The danger increases as those small, separate record keeping systems converge into national citizen databases [7].

Undoubtedly, technology relative to data protection, information sharing protocols, technological standards, and human rights legislation will determine the level of protection for the individual. With the inarguable increasing globalization, the daunting question remains as to who will ultimately define the rules globally as well as who will hold the keys to the information protocols and processes to dynamically guard against the excessive and intrusive collection of personal data. There is a cry for international standards technologically, such as US Secretary of Homeland Security Tom Ridge calling for common international standards for biometric identity recognition technology, and saying in January 2005 that they are essential for travel safety.

5.2 Secondary Concern: Data Security

When reviewing an identification system, RSA Security (2002) outlines four key elements of a privacy policy: Notice, Choice, Access and Security. Notice defines that users must be able to receive previous notification of information practices; Choice defines that users need to be in a position to provide specific consent to the gathering and use of information pertaining to them; and Access states that users need to have the ability to access their own personal information whenever needed. Relative to the fourth requirement of Security, RSA states that users need to have assurance that the organization has taken and is taking measures to prevent unauthorized access to and use of their personal information. Yet, the concern with tracking at such individualized levels that reduce or eliminate anonymity requires an additional unanswerable question as to not only who will be authorized to access the information currently, but also who may have access to wield the control in the future.

Issues in data security have yet to be solved as seen recently when the European Union (EU) cited data security and interoperability of reading devices as issues requiring resolution prior to moving forward with biometric passports, and thereby asking the U.S. to extend the current deadline of biometric-RFID passports from October 2005 to August 2006. The EU defined the most serious issue as the protection of the data that would be housed on a contactless chip. There exists a threat that unauthorized readers could access the data without having the necessary security mechanisms protecting access to the chip as well as the radio transmission when activated. Solutions have been posed such as a foil barrier within which the passport would remain housed until presented at required sites.

Yet even the standardization of the actual biometric data that would be collected has not yet been agreed upon by the key players, with the EU deeming fingerprints to be compulsory for obtaining a passport and the UK determining face scans as a requirement that is to be housed on the RFID chip and thereby currently abandoning the previously stated requirement of face, iris and fingerprint data.

Although there is a push to develop technology that will provide data security methods that will ensure the protection of the information as well as the privacy of the individual, until these obstacles are extensively overcome, implementation is likely to be inhibited.

6. Survey Data: Implantable RFID Chips as a Biometric Identification Method

With the US Food and Drug Administration approving the practice of injecting humans with tracking devices for medical purposes in 2004, companies such as Applied Digital are planning to provide complimentary scanners to hundreds of trauma centers. Interestingly, this implantable chip is being marketed as a lifesaving device.

Data in the past has revealed that the majority of the public is unwilling to implant a chip into the body. Applied Digital states that their own study confirmed most people find implantable chips "creepy" and the study commissioned by NJIT in 2002 showed that over three-fourths of respondents were unwilling to implant a chip within the body [9].

Yet landscape is changing, showing the increasing societal acceptance of technologies such as biometrics and RFID. There are aligned motivational forces for social acceptance of these methods exclusive of implantable chips. The subsequent question is if there are similar motivational forces that would create the impetus for the societal acceptance of the same data and same methods now deposited in a much safer place: the human body.

In reviewing data from the studies relative to the social acceptance of identity management utilizing biometric and RFID methods, it became apparent that there were aligned motivational drivers for compelling acceptance: fighting terrorism, reducing identity theft, security and convenience. Therefore, a sample survey was done to compare the previously determined key motivational drivers of acceptance of biometrics and RFID usages to those motivation drivers when considering implanting a chip.

6.1 A Sample Survey

The topic of this sample survey was to measure perception based on various uses of biometric technology as well as implantable RFID chips in the human body as an enhanced biometric method.

6.1.1 The Method, Subjects and Instrument. The survey was distributed in two colleges in Massachusetts and across approximately twenty majors or concentrations. The survey was distributed to students and the following verbiage was included on the top of the survey preceding the eleven questions: "Biometrics refers to the automatic identification of a person based on his or her physiological or behavioral characteristics, such as fingerprints, facial recognition, or voice signature. This method of identification is being considered over current methods involving passwords and pin numbers for various reasons. In October 2004, the FDA approved an implantable microchip for use in humans. The tiny RFID chip, which is implanted in the body, is being marketed as a lifesaving device. If you're brought to an emergency room unconscious, a scanner in the hospital doorway will read your chip's unique ID. That will unlock your medical records from a database, allowing doctors to learn about your penicillin allergy or your pacemaker." The survey was completed anonymously.

The average age of the respondent was 21 years. The subjects represented both full-time and part-time four-year college students, with the gender categorization being 62% male and 38% female (n=141).

The instrument consisted of basic demographics in addition to questions adapted from an ITR Collaborative Research project funded by NSF and entitled "Biometrics – Performance, Security and Societal Impact" [1]. Nine of the eleven questions utilized were formatted to measure how willing an individual would say that they would be relative to utilizing a biometric method and/or an implantable chip for reasons such as: boarding an airplane, entering governmental buildings such as historical landmarks or nuclear facilities, obtaining a credit card, obtaining a US Passport, ensuring against identity theft, ensuring greater safety and security for the individual and his or her family, as a potential lifesaving device, and as a method for national security. Subsequently, two final questions were used to identify levels of concern and drivers correlative to the preceding nine questions.

6.1.2. Findings. Relative to the use of biometric methods in functions such as boarding a plane, entering governmental buildings and obtaining a passport, the data in this survey was analogous to the Cap Gemini study depicting favorable responses at 45% for the former and 42% for the latter [18].

As seen in Table 1, respondents in this survey were most willing to enroll biometric identifiers into the United States Passport system with almost half of respondents willing. Conversely, respondents were least willing to enroll biometric identifiers into a system to obtain a credit card with results showing nearly two-thirds of respondents unwilling.

The study commissioned by NJIT in 2002 revealed that 78.3% of respondents were unwilling to implant a chip in their body [9]. Yet in the sample survey, response percentages reveal less than half of respondents are

unwilling to implant a chip; one-third of respondents were willing.

Data in this survey indicates that respondents are least likely to say that they would be willing to implant a chip in their body as method for national security with half of respondents unwilling.

TABLE 1

		Not at all & Somewhat unwilling	Very & Somewhat willing
Q #1	Biometrics: Airplane	42%	44%
Q #2	Biometrics: Govt. Buildings	43%	45%
Q #3	Biometrics: Obtain Credit Card	64%	17%
Q #4	Biometrics: Passport	39%	47%
Q #5	Implantable: Identity Theft	55%	34%
Q #6	Implantable: Anti-terrorism	50%	31%
Q #7	Implantable: SS for Family	44%	43%
Q #8	Implantable: Lifesaving Device	42%	44%
Q #9	Implantable: National Security	50%	32%

Overall, respondents were most willing to implant a chip in their body as a lifesaving device, which was implied as "being brought to an emergency room unconscious and a scanner in the hospital doorway will read your chip's unique ID that will unlock your medical records from a database allowing doctors to learn about your penicillin allergy or your pacemaker." It should be noted, though, that respondents were almost equally unwilling.

The areas rating highest relative to those saying that they are "very willing" to consider implanting chips were for the purposes as follows: "as a potential lifesaving device" or "to ensure the safety and security of me and my family".

Regardless of the willingness exhibited in enrolling biometric data to ensure against identity theft, over half of respondents in this survey were unwilling to implant a chip in the human body to ensure against identity theft.

Those respondents who remain "undecided" on the methods such as biometrics/or and implantable RFID chips and the various uses represented, averaged an approximate 15% of those surveyed. The survey did not measure reasons why the respondents might choose "undecided".

The authors recognize that this survey is an exploratory study and that much more additional data would be needed to generalize the results of this survey.

8. Summary and Conclusions

With a void in the public awareness of these technologies, there is a current thrust from advocates of identity management and tracking systems to fill the vacuum with information highlighting the benefits and conveniences. Through the surveys reviewed, as well as the sample survey, the data shows that is a robust percentage undecided. Although this sample survey did not measure the motivational forces as to why an average of 15% of the respondents chose "undecided", perhaps lack of comprehensive knowledge may have been a veritable factor. Relative to the sample survey, one might consider that the "undecided" respondents (averaging 15% across all usages) represent a robust swing vote relative to an increase in social acceptance, when considering that the acceptance of certain uses is divided somewhat equally.

When considering potential drivers, it is imperative to note that the sample survey data corresponded to previously done surveys relative to biometric methods.

The data relative to implantable chips seems to exhibit a higher societal acceptance when questions were presented not by the intended use, but rather by a perceived benefit. When asked to choose the one most important reason why you might be willing to implant a chip, willing respondents increased by 4%, bringing the results to almost half of all respondents indicating that they would say they would consider an implantable chip "for the overall safety and security of me and my family" or "as a lifesaving device". When presented from the perceived advantages, there was a drop in resistance, thus depicting a reduction from over one-quarter to under one-quarter of respondents citing "no reason would make me willing" to consider an implantable chip.

When bearing in mind questions corresponding to areas of concern, the survey data was correlative to the BIGresearch and Artafact LLC Consumer RFID Buzz Survey where 63% of respondents concerned with privacy relative to RFID technology [3]. In the sample survey, over half of respondents in the sample survey consider "privacy concerns" as the area of primary concern when considering biometrics and/or implanting a chip. In addition and relative to privacy, almost one-third of respondents were concerned with "not knowing who is tracking me". A lesser minority expressed their chief area of concern to be "potential misuse of my personal data".

As evidenced by the sample survey, as well as the national and international studies reviewed by the authors, there are evident drivers for the acceptance of current biometric and RFID methods such as fighting terrorism, reducing identity fraud, security and convenience. Ensuring methods of accurate identification of individuals is the key in overcoming these desired outcomes.

Presently, individuals undoubtedly struggle to provide their unique identity with an overabundance of number sequences, passwords, photo cards, or electronic gadgets so as to function in a 24-hour period between the everyday tasks performed or activities enjoyed. Merging

information into once source seems as predictable as the programmable remote control now available to run the host of equipment now typical in the home. Yet, does an easily stolen or lost card or wristband solve the problems or create a myriad of new ones? It would seem predictable that eventually there would be an identification and processing method incapable of being stolen or altered, yet also unique to the individual and proficient enough to house key data that is easy accessible.

Perhaps after the public is accepting of one safe and secure multipurpose identity card that will provide the convenient and secure means to any service or transaction process expediently and reliably, the next push will be toward a method that could never be stolen or lost. A solution just might be found in a newly created pattern-recognition identifier, such as an implantable chip, called an implanted "feature vector" and housing electronically the specific physiological or behavioral characteristics along with a unique identification number.

By this point though, the public may have gradually rescinded the control over when and by whom the various parts of us can be sensed by others [14]. If the environment within which society is making the decision to embrace an implanted identification device happens to be one where recent events have validated the feared threats or breaches in the safety and security of the individual and his or her family, the individual may very well perceive the decision as if it were a life or death option. Thus, we see the traceable feature vector enter with a unique implanted identification number housing key data in the form of an implantable chip. Yet the true looming threats remain in the unanswered query as to who will hold wield the control of the information now…and well into the future.

10. References

[1] Acuity Market Intelligence (2005) "ITR Collaborative Research Project -Biometrics: Performance, Security and Societal Impact". April 2005. http://acuity-mi.com/UofP_Page.html

[2] J. Best. (2004) "44,000 Prison Inmates to be RFID-chipped". August 2, 2004. http://networks.silicon.com/lans/0,39024663,39122811,00.htm

[3] BIGResearch., (2004 & 2005) "RFID Consumer Buzz Survey", April 1, 2005. http://www.bigresearch.com/rfid.htm

[4] Chirillo, J., and Blaul, S. (2003). *Implementing Biometric Security.* Wiley Publishing, Indianapolis.

[5] J. Collins, "Consumers Voice Opinions on RFID", *RFID Journal*, February 2, 2004. http://www.rfidjournal.com/article/articleprint/781/-1/1

[6] EPC Global (2005) "About EPC Global Network". March , 2005. http://www.epcglobalinc.org/

[7] I. Giesing. (2003) "Biometrics" March 2005. http://upetd.up.ac.za/thesis/available/etd-01092004-141637/unrestricted/05chapter5.pdf

[8] A. Gilber. (2004) "Theme Park RFIDs Kids for Safety". September 15, 2004. http://networks.silicon.com/lans/0,39024663,39123979,00.htm

[9] S.R. Hitz, H. Han, V. Biller, (2003) "Public Attitudes towards a National Identity "Smart Card": Privacy and Security Concerns". March 1, 2005. http://csdl.computer.org/comp/proceedings/ hicss/2003/1874/05/187450139aabs.htm

[10] Library of Congress: Thomas Legislative Information (2005). "Bill Number H.R.418 for the 109th Congress" March, 2005. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.418:

[11] G. Magnuson, P. Reid (2005). "Privacy and Identity Management Survey" April 2005. http://www.eds.com/services/innovation /downloads/privacy_survey.pdf

[12] K. Murphy, "Zipping through airport security", *Businessweek,* September 6, 2004, p 106.

[13] Nabbali, T. and Perry, M. "Going for the Throat: Carnivore in an Echelon World, Part II." *Computer Law and Security Report,* Vol. 20-2, 2004, pp. 84-97.

[14] R.B. Parker, "A Definition of Privacy"*, Rutgers Law Review,* Vol 27, 1974, pps 275-29.

[15]Ribaric, S., Ribaric, D. and Pavesic, N., "Multimodal Biometric User-identification System for Network-based Applications", *IEE Proceedings Online: Vision, Signal and Image Processing,* p. 150.

[16] B. Schechner. (2004) "Explosive Biometrics Push Homeland Security into Consumers' World". November 1, 2004. http://www.abiresearch.com/abiprdisplay.jsppressid=354

[17] SEARCH: The National Consortium for Justice Information and Statistics (2005). "Public Attitudes toward the Uses of Biometric Identification Technologies by Government and the Private Sector" September 2001 and August 2002. http://www.search.org/files/pdf/Biometricsurveyfindings.pdf

[18] A.J. Vethman (2005) "RFID and Consumers". March 1, 2005. http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

[19]J. Woodward, N.M. Orlans, P.T. Higgins, *Biometrics: Identity Assurance in the Information Age*, McGraw-Hill/Osbourne, New York.

[20] X. Yuan, S.C. Hui, H.K. Leung & Y. Gao, "Towards a BioAPI Compliant Face Verification System", *Computer Standards and Interfaces*, August 2004, Vol. 26, pp. 289-299.