1

Biometrics: Identification and Verification for Tomorrow?

Robert Arthur Richardson and Travis Thrush

Biometrics Overview

Rene Ramon Sanchez knows all too well of the problems that can arise for an individual living in a society that blindly trusts biometric data. Sanchez, an auto-body worker, was misidentified by the courts as Leo Rosario, a known drug dealer. Due to a clerical error, Sanchez's fingerprints, one of the most indisputable biometric identifiers, were confused with those of Leo Rosario. In one of the court cases that followed, the judge told Sanchez, "The general rule is, the prints don't lie. If you got the same prints that Leo Rosario has, you're Leo Rosario. And there's nothing I can do about it" (Weiser 2004, p. 2). Sanchez had been placed in the difficult situation of proving to the government that he was not Leo Rosario. After spending two months in custody and being threatened with deportation, Sanchez decided to sue the state, and only then did the problem begin to be resolved (Weiser 2004). This man's story demonstrates the infallibility with which society has come to view biometric technologies like fingerprinting. In this case, the system relied so heavily on the accuracy of the fingerprint data in question, that Sanchez spent six years of his life trying to clear up the confusion surrounding the state's clerical error.

In the wake of the September 11th tragedy, there has been a renewed attention to biometrics as a security measure. Supporters of biometric technologies view it as a "silver bullet" for battling terrorism on the home front, as well as a new and highly secure form of personal identification and verification. Critics of biometric technologies worry that, without sufficient attention to privacy protection, it is likely that

these technologies will be used in a way that is dangerous to civil liberties (Abernathy 2004). This chapter will begin by answering the question of what exactly are biometrics and why they have the potential to affect the lives of everyone. The chapter will then take a closer look at a single biometric technology, Facial Recognition, and address the challenges and conflicts it presents, and the ethical implications of these challenges.

Biometrics: Identification & Verification of Tomorrow?

So what is biometrics? Biometrics has been defined by the FDA Office of Regulatory Affairs as:

> A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable (Schultz 2001, p. 2).

The most common forms of biometric ID are the face, fingerprints, hand geometry, handwriting, iris, retina, vein, and voice. The use of biometric technology falls into two categories. The first category is verification. Biometric data can be used to verify that a person is who he or she says they are by comparing the previously stored characteristic to the fresh characteristic provided. This is referred to as a "one-to-one match." The second category is identification. Biometric data can be used to identify an individual where the fresh characteristic is compared against all the stored characteristics. This is referred to as a "one-to-many match" (Privacy International 2003, p. 14).

While it is true that biometric awareness has grown following September 11th, biometrics is really nothing new -- fingerprinting has been going on for decades. However, what is new is biometric technology. New biometric technology attempts to automate and enhance the identification and verification process by using advanced computer algorithms. It is important to note that these algorithms have not been fully perfected and may never be. This opens the possibilities for one of two things: a false match (incorrectly matching a subject with someone else's reference sample) or a false non-match (failing to match a subject with his/her own reference sample) (Abernathy 2004). Nevertheless, biometric schemes are being implemented around the world because they promise to do what humans cannot: quickly and accurately identify and verify individuals. They also enable the use of previously unused biometric characteristics such as the eye retina through retinal scanning. Many people pose the question of whether or not society really needs a better form of identification and verification. To better understand this question, one must compare biometrics with today's dominant token system.

Besides personally recognizing someone, or being identified by a trusted third party, the only other technique for identifying a person, according to the Electronic Frontier Foundation, is through the use of a "token." Tokens come in two basic forms: Knowledge Tokens and Physical Tokens. Knowledge tokens are passwords, Personal Identification Numbers (PIN's), or knowledge of personal data such as your mother's maiden name. Physical Tokens are ID cards, passports,

chip cards, or plain old keys (Abernathy 2004). Today's forms of identification and verification are dominated by the token based system. Unfortunately, the token based system has a problem. Current systems verify the token but often don't verify that the possessor of the token is actually the token's owner. Prime examples are online credit card transactions. Online retailers will verify a username, password, and a credit card (all tokens), but not whether the owner of the credit card is actually the person using the credit card to make the purchase.

The advantage of biometrics is that the attributes measured cannot ordinarily be lost, stolen, loaned, or forgotten so the possessor of the identifier is ordinarily always the owner. "As the level of security breaches increase, and transaction frauds increase, the need for highly secure identification and personal verification technologies is becoming apparent. Consumer and business trust in these electronic transactions is essential to the healthy growth and advancement of the global economy" (Abernathy 2004, p. 1). Biometrics could effectively replace the token system, or when combined with token systems such as smart cards and encryption keys, could greatly reduce the vulnerabilities of the token system.

It appears that this is the growing consensus among private and public sectors in the U.S. and the world. In the private sector, computer manufacturers have begun building biometric readers on new computer systems as businesses begin demanding more secure forms of verification for their employees. As of 2003, France and Germany were reportedly testing equipment that put fingerprint information into credit cards (Privacy International 2003, p. 14). When it comes to the public sector, among the suggestions in the report from the 9/11 Commission investigating the events on September 11, 2001, was a call for the adoption of biometric technologies in US security measures. Hence, the Enhanced Border Security and Visa Entry Reform Act of 2002**,** Sec. 303(b)(1) was created, which required that only "machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" be issued to aliens by October 26, 2004.

In another example, on October 25, 2004, News.com reported that the U.S. was moving forward with plans to issue new high tech passports in 2004 that incorporate facial recognition technology despite privacy concerns and possible technical problems. Furthermore, it appears that biometric technology is favored over "tokens" by individual citizens. The authors of this chapter performed a recent survey of individuals that posed questions pertaining to the topic of biometrics. When asked the question, "which would you rather use to access your private information (ATM, email account, etc.) on a daily basis?", 67% of those questioned said that they would rather use their fingerprints, retina, face, or voice as opposed to 33% who said the would prefer to continue using passwords and PIN numbers.

There appears to be overwhelming support for implementing biometric technologies into our everyday lives. So what about the critics who fear that biometrics would erode our privacy? Are supporters of biometric technologies ignoring the full picture? Perhaps a closer look at a single biometric technology, facial recognition, can help to answer these questions.

Facial Recognition: A Closer Look at Biometric Technology

Facial Recognition Technology (FRT) systems recognize a person by using one of several possible methods, all of which emphasize parts of the face that are not easy to alter such as the areas around the cheekbones, the upper outlines of the eye sockets, and the sides of the mouth (Speir 2002). While receiving much hype as one of the newest and most promising security related applications of biometrics, it remains to be seen whether FRT will be able to deliver on the promises made by its promoters.

FRT has been shown to work well in laboratory settings. However, for systems implemented in public areas, the results have been more dubious. Some government agencies, including the Immigration and Naturalization Service have already tried and discarded FRT as a viable security measure (Q&A on Facial Recognition 2002). Faults with systems placed in the public surveillance arena include poor system performance when cameras are off by more than 15 degrees in relation to the subject (Abernathy 2004), and less than human performance when accounting for changes in lighting conditions and changes to faces themselves (Phillips 2000). These are significant technical barriers to be overcome, in addition to the public scrutiny that this type of public surveillance/security system would have to overcome in order to be widely accepted.

A PAPA analysis is effective at taking a deeper look at the issues surrounding FRT. The PAPA form of analysis, created by Richard Mason, is one that looks at four ethical dimensions: Privacy, Accuracy, Property, and Access.

Privacy

Biometric applications like FRT are slowly and unbeknownst to most, entering into the everyday lives of the citizens of the world. One day, FRT technology could pervade the very fabric of society. Left unchecked, this technology could begin to affect society in ways only imagined in sci-fi novels. To illustrate this point, reflect on the once unimagined ways that Social Security numbers are now used throughout everyday life in the U.S. Social Security numbers today are used as personal ID numbers by numerous organizations including universities, businesses, and credit card companies. At the advent of this system, many of these uses were never fathomed nor intended. Now imagine that all this time, you were using your face rather that your social security number. When combined with existing public surveillance systems, the potential effects of widespread FRT are apparent.

It is for this reason that effective regulatory legislation be put in place before FRT systems are widely used. Otherwise, these systems could become the "eye in the sky," tracking *and* recording one's every move. Putting strict regulations in place before FRT is widely used is the key to reigning in such a potentially useful, yet privacy threatening technology.

Accuracy

By definition, biometric technologies depend on measuring multiple, repeatable actions or characteristics of the subject being

identified by a particular biometric system. This makes the accuracy of the biometric data involved in any biometric system the most important element in maintaining the integrity of the system and the trust of the users. Society is already feeling the weight of the inaccuracy of the huge amounts of data being stored today. Because biometric data can be so complex it may be difficult to maintain its integrity. As the problems encountered by Rene Ramon Sanchez demonstrate, the cost to an individual is huge when the data in question is in error. Considering that most of the proposed uses and benefits of newer biometric technologies are in the field of security, the importance of data accuracy is magnified. But the challenges of maintaining the accuracy of biometric technology do not end there. Most biometric data changes over time as people age or are injured. Not only will biometric data have to be extremely accurate, but FRT systems will require constant updating to reflect the changes to its subjects.

Which parties involved in any biometric system should be responsible for maintaining the accuracy of the data? If a system is put into place in which the responsibility of maintaining data accuracy is placed on the subjects of the system, the security fallibilities are obvious. How can a widespread biometric security system be implemented without some kind of separate organization devoted not only to the maintenance and accuracy of the information, but also to the continued collection of data in order to keep up with changing biological characteristics of the subjects of the system? There are other aspects to be dealt with when considering the issue of biometric data accuracy. While biometric technologies are being touted as a solution to many current security issues, the fact remains that many of these technologies can be compromised. A good example is the supposedly invulnerable technology of fingerprinting. Ever since fingerprinting has been widely used, people have been "erasing" their fingerprints (by burning or sanding them off), with the purpose of evading identification by fingerprinting systems. While FRT has been promoted as the next best advancement in biometrics, one cannot help but notice the concurrent popularity and advancements in the field of plastic surgery. It is easy to see people engaging in the same type of devious behavior that is used to defeat fingerprint identification in order to defeat FRT. A simple surgical change to a person's face could effectively nullify millions of dollars in investments in an FRT system. The point is that no matter what the latest and greatest technology is, it is only as good as the system used to implement it. If someone desires to beat the system badly enough they will find a way. Maintain data accuracy would be a large challenge when faced with the situations presented above. This could seriously undermine FRT's effectiveness as a security application.

Property

Ancient cultures in South America and the Far East used to believe that if one's picture was taken, his or her soul could be stolen. With the widespread use of photography today, this view has become rare. However, as FRT becomes more popular today, the question emerges: "Who owns your face?" It is only a matter of time until advancements enable FRT and public surveillance systems to be combined. Depending on the legislation in place regulating these technologies,

citizens all over the world within the scope of surveillance cameras, could be identified through FRT systems, and potentially tracked wherever they travel. For now, a person who does not want to be tracked or recognized by a camera linked to an FRT system simply needs to cover their face. In the future, however, these types of systems will not be so easily evaded. With the advent of new 3-D image-based facial recognition systems, and ever advancing feats in the realm of infrared photography, FRT will be used more effectively (Anonymous 2004).

Accessibility

The lack of intrusiveness of FRT is a benefit, but this is also what makes the technology such a potential threat to privacy. For example, a person may never know if their face has been captured by an FRT system. With this in mind, someone cannot be reasonably expected to keep track of the databases in which their image exists, who accesses it or how it is used. If the face becomes a primary identifier, as fingerprinting is today, this could present problems. Currently people have a reasonable amount of control over and knowledge of who has their fingerprints, but if FRT use becomes widespread, people may lose control over their primary identifier - their face. Depending on the amount of FRT data access granted to public and private entities, a person's expectation of privacy could be drastically changed. FRT systems could potentially be used to track every building, park, and road intersection a person was to pass during the course of their everyday lives. With the U.S. government's recent legislation of the Patriot Act, this possible use of FRT seems all too real. Imagine a not too distant future when FRT systems are on every block. If the government had even the slightest suspicion that a person could be involved in terrorist activities, the government could track everywhere that person's face had been logged by an FRT system. For some people this is a scary thought, but for others, the applications of FRT towards the prevention of criminal activity are beneficial.

As previously illustrated with the concerns regarding privacy and FRT, the most pressing issue about access to biometric data is clearly delineating how much access the government and corporations should have to biometric databases. This begs the question, "How much privacy should one be willing to give up in order to achieve personal safety?" In the opinion of Benjamin Franklin, "They that can give up essential liberty to obtain a little safety deserve neither liberty nor safety." However, a post-9/11 survey, discussed in more detail later, indicates that the opinions of most Americans seem to differ greatly from those of Ben Franklin.

Facial Recognition Technology: An Ethical Analysis

The PAPA analysis has pointed out the inherent problems and ethical challenges facing FRT. These problems are similar to many of the problems faced by other biometric technologies. All of these problems pose one underlying question: What constitutes the best method of identification and verification in our society? The question is one based upon ethical dilemmas. The answer requires an in-depth ethical analysis. And yet, in the end, there most likely will not be a

definitive answer. At the very least, a better understanding of the multiple underlying ethical perspectives can be achieved.

Before beginning this ethical analysis, a review of the basic normative ethical theories is necessary. Normative ethics is a set of premises used to decide whether an action or decision is right or wrong (Wood-Harper 1996, p. 71). While there are many ethical theories, this chapter will focus on the three most common and well-known: ends-based thinking, rule-based thinking, and care-based thinking.

Ends-based thinking, also known as utilitarianism, is categorized as teleological thinking. It basically says "do whatever produces the greatest good for the greatest number." It is essentially a cost-benefit analysis, determining who will be hurt and who will be helped and then measuring the intensity of that hurt and help. This theory form is the staple of public policy debate – most legislation is crafted with the utilitarian mindset (Kidder 2004).

Rule-based thinking is often associated with the German philosopher Immanuel Kant and categorized as deontological thinking. Kant called this ethical principal "the categorical imperative." The theory simply says "follow only the principle that you want everyone else to follow." Said another way, "act in such a way that your actions could become a universal standard that others ought to obey." It is important to note that this mode of thinking is in direct opposition to utilitarianism. It believes that "ends-based thinking" is flawed because one can never fully imagine the entirety of consequences associated with an action (Kidder 2004).

The principle of care-based thinking is putting love for others first. This is considered synonymous with the Golden Rule: "Do to others what you would like them to do to you." Philosophers refer to this ethic as reversibility. In other words, test your actions by putting yourself in another's shoes and imagine how you would feel as the recipient rather than the perpetrator of your actions (Kidder 2004).

When people think of an ethical discussion, they often think of the disorganized debate that occurred in their college ethics course, or the unfortunate heated debate between extended family members over a holiday dinner. These discussions are typically characterized by a chaos of thoughts and opinions. They tend to be the farthest thing from organized, rational discussion. This analysis hopes to avoid this chaos so that the reader can make sense of the web of ethical perspectives. The analysis will follow a series of precise steps based on the stakeholder analysis and the assumption surfacing approach used by Mitroff and Linstone (Wood-Harper 1996, p. 73). The analysis involves five key steps:

1. Identify the stakeholders in the situation who possess ethical perspectives.
2. Identify their dominant perspective. If no dominant perspective exists, identify the top dominant perspectives as different stakeholders.
3. Construct an ethical conflict web, mapping different perspectives.

4. Identify those strands of the web where no significant conflict may be assumed to exist. These may be removed from the model.
5. Concentrate on those strands where conflict does exist. Use a technique of conflict resolution to achieve the "good" for the system (Wood-Harper 1996, p.73).

Step 1: Identify the stakeholders. A stakeholder is any individual, group, organization, or institution that can affect, as well as be affected by an individual's, group's, organization's, or institution's policy or policies. The first and most important stakeholder is the individual person. After all, they are the source of any biometric characteristic. A second stakeholder is society as a whole since it is composed of all individual stakeholders. A third stakeholder is corporations. Corporations are the entities that are developing the technology to make biometric identification and verification a reality. Corporations will also be utilizing the technology for their own means of verification. A fourth stakeholder is the government as it will undoubtedly use the technology for identification and verification in addition to providing regulations pertaining to its use.

Step 2: Identify the dominant ethical perspectives. For the individual, there are two dominant perspectives. On one hand, individuals are very concerned about their security and the threat of terrorism. If FRT technology could better protect the homeland, then that end justifies the means which may invade levels of privacy for the individual. This ethical perspective parallels ends-based thinking. On the other hand, individuals are very concerned with the potential of FRT to erode their levels of privacy regardless of the potential for better security to prevent terrorism. For this individual, the ends don't justify the means and therefore their ethical perspective is that of "rule-based thinking."

The perspective of society is largely dependent on the dominant opinion of the individuals that compose that society. The National Consortium for Justice Information and Statistics commissioned a biometrics opinion poll in the United States in two waves. The first occurred Sept. 18-30, 2001, shortly after the terrorist attacks, and the second, Aug. 15-18, 2002. Although there were slight declines of acceptance over the year, public support for biometric use by law enforcement for antiterrorist or crime prevention remained high (86 percent in 2001 and 80 percent in 2002) (Sarkar 2002). Based on this data, one could conclude that in the application of FRT for identification, the predominant ethical perspective of FRT in society would be ends-based thinking. People are willing to give up levels of their privacy for an end result of increased security.

When analyzing the corporation, it is most effective to view the corporation as an individual. Viewing it as an individual, one can conclude that the ultimate goal of the corporation is to be profitable. Corporations producing FRT technology have an interest in the successful implementation of the technology because it means more revenues. Corporations also have an interest in FRT because they are interested in enhanced security measures to protect their intellectual property. In light of this, the dominant ethical perspective of the

corporation is "ends-based thinking" in order to maximize the good for itself.

We accept the government's ethical perspective to be that of ends-based thinking as well. As stated earlier, ends-based thinking tends to be the dominant reasoning behind most legislation. While the cost of implementing FRT could be a reduced level of anonymity for individuals, this cost is overcome by the benefits FRT bestows on the individuals in society. On the application of identification, FRT could more effectively identify terrorists and remove them from society, increasing the safety of individuals. On the application of verification, FRT could reduce identity theft and its associated problems through improved verification.

Step 3: Construct an ethical conflict web, mapping different perspectives. Figure 1 below provides a visual representation of the conflicting ethical perspectives between the stakeholders in our analysis. The two lines drawn between the individual, and the corporation and government are a representation of the conflicts between the rule-based perspective of individuals and the ends-based perspective of the corporation and the government. The same conflicts are paralleled between society and corporation and between society and government. These conflicts would exist if the majority of individuals in society developed the rule-based perspective. Finally, the line between the government and the corporation is a representation of the conflict between the government's attempts to lookout for the rule-based individual through policies that may conflict with the end-based perspective of the corporation to benefit its self.

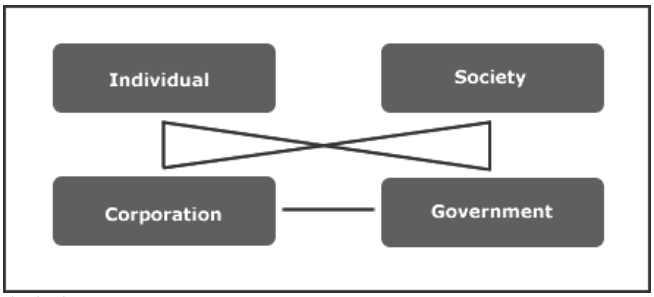

Figure 1: Ethical Conflict Web

Step 4: Identify those strands of the web where no significant conflict may be assumed to exist. These may be removed from the model. All the conflicts existing in the web diagram are significant and therefore should remain in the web for further consideration.

Step 5: Concentrate on those strands where conflict does exist. Use a technique of conflict resolution to achieve the "good" for the system. The conflict web makes it clear that there is one major conflict when it comes to answering the question posed at the beginning of this analysis: What constitutes the best method of identification and verification in our society? This conflict is between the "rule-based thinking" of the individual and the "ends-based thinking" of the government and corporations.

Fortunately, the U.S. government is a democracy and thus the government and corporations, ultimately governed by the government, are held accountable by the individual citizens of the governed society. In order to resolve this conflict, society should require the government to develop legislation and policy that protects the privacy concerns of the "rule-based" individual in society. At the same time, these policies set forth by the government can impede the "ends-based" goals of the corporations and thus create the conflict between government and corporation seen in Figure 1. In the eyes of certain individuals, the government holds the interests of the corporation higher than those of its citizens. On the flip side, the government needs to protect the corporations because they arguably drive the success of our economy, the success of society, and hence the success of the individual. Thus there is no definitive answer to these complex conflicts. The process becomes a legislative balancing act for the government to manage the interests of individuals, corporations, and itself. The authors of this chapter believe that while corporations my drive the success of the economy, success of society, and hence success of the individual, it is the individual that the government must hold at the highest priority when forming acts of legislation to govern biometrics initiatives. While earlier in the ethical analysis, it may have been effective to view corporations as individuals, the truth is that corporations are composed of individual citizens. If the rights and liberties of the citizens are trampled, the corporation is inevitably affected as well.

Conclusion

Biometrics has the potential to change the everyday lives of people all over the world. As technology advancements move forward and biometric applications become viable, the questions surrounding biometrics will change from focusing on the actual technology to how the technology is used. The effects of biometric applications on everyday life will be increasingly amplified as biometric technologies are combined with existing and upcoming identification technologies such as Radio Frequency Identification (RFID) and public surveillance systems. If specific guidelines are put into place in order to regulate the ethical usage of biometric technologies, society could greatly benefit from its implementation in everyday processes. However, if guidelines are not put in place, the privacy rights of citizens in society are at risk. As with many laws and regulations in the U.S. today, regulations regarding biometrics will be forced to constantly evolve as new uses for biometric technologies are envisioned and put into everyday practice.

Works Cited

Abernathy, William, and Tien, Lee. "Biometrics Who's Watching You." *Electronic Frontier Foundation. Defending Freedom in the Digital World*. EFF. October 3, 2004 < http://www.eff.org/Privacy/Surveillance/biometrics.html>.

"An Introduction to Biometrics" *The Biometrics Consortium.* October 3, 2004 <http://www.biometrics.org/html/introduction.html>.

Anonymous. "Are CMOS & Image Analysis The Next Trends?" *Security.* September 2004. Accessed November 1, 2004. Vol. 41, Iss. 9; p. 40-42.

"Biometrics Context / Issues" *Acsys Biometrics Corp.* October 3, 2004 <http://www.acsysbiometrics.com/knowledge_context.html>

Kidder, Rushworth. "How Good People Make Tough Choices." *Institute for Global Ethics*. September 7, 2004. <http://www.globalethics.org/pub/toughchoices.html>

Phillips, P. Jonathon, Martin, Alvin, Wilson, C.L. Pryzbocki, Mark. "An Introduction to Evaluating Biometric Systems." *FRVT Face Recognition Vendor Test.* February 2000. Accessed October 3, 2004 <http://www.frvt.org//DLs/Feret7.pdf >.

"Privacy and Human Rights 2003: Threats to Privacy." *Privacy International.* August 12, 2004. <http://pi.gn.apc.org/survey/phr2003/threats.htm>

"Q&A on Facial Recognition." *ACLU. American Civil Liberties Union. Freedom Network.* 2002. October 3, 2004 <http://archive.aclu.org/issues/privacy/facial_recognition_faq.html>

Schultz, William B. United States Dept. of Health and Human Services. United States Food and Drug Administration. Office of Regulatory Affairs. *Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures Final Rule Published in the Federal Register.* June 1, 2001. Accessed October 3, 2004 <http://www.fda.gov/ora/compliance_ref/part11/frs/background/11cfr-fr_02.htm>.

Sarkar, Dibya. "Biometrics awareness still low." *Federal Computer Week.* November 6, 2002. Accessed October 25, 2004. <http://www.fcw.com/geb/articles/2002/1104/ web-survey-11-06-02.asp>

Speir, Michelle. "The New Face of Security." March 4, 2002. *Federal Computer Week.* Accessed October 5, 2004. <http://www.fcw.com/fcw/articles/2002/0304/tec-face-03-04-02.asp>

Weiser, Benjamin, "Can Prints Lie? Yes, Man Finds to His Dismay" May 31, 2004. *The New York Times.* Nov. 3, 2004. <http://www.nytimes.com/2004/05/31/nyregion/31IDEN.html?hp>

Wood-Harper, A.T., Steve Corder, J.R.G. Wood, and Heather Watson. "How We Profess: The Ethical Systems Analyst." *Communications of the ACM.* March 1996. Vol. 39, No. 3.