

“The Biometric Quarterly”

4th Quarter, 2009

Brought to you by BiometricNews.net

www.biometricnews.net

publisher@biometricnews.net

630-261-5677

Welcome to the 4th Quarter, 2009 Edition of The Biometric Quarterly. In this quarter’s Newsletter, you will find an exciting array of topics in Biometrics, such as:

- *Biometric Bits Section:*

“An introduction to Biometrics- Part II”: In this quarter’s issue, we continue our theme of reviewing the Biometric Technologies which are available today, the differences between Physical Biometrics and Behavioral Biometrics, and some of the major scientific components of Biometrics which are important to consider when implementing a Biometric System at your place of business.

- *Biometrics Editorial Review Sections:*

In this Quarter’s Newsletter, we take a global perspective of Biometrics, from two countries, literally halfway around the world from each other: The United States and South Africa.

With regards to the United States, we examine a country which is the most technologically advanced in the world, but yet the adoption rate of Biometrics amongst the public is probably among the lowest when compared to the rest of the world. A lot of this has to do with the very low perception of Biometrics, and we examine the various reasons why.

Next, we take you to the other side of the world, to the African Continent, specifically South Africa. This is a country where even the smallest item is considered to be a luxury. When compared to the United States, the adoption rate and perception of Biometrics is growing by leaps and bounds. A primary reason for this is that Biometrics is considered almost a necessity in order for each and every citizen to be counted and cherished as an individual, where the value placed on life is much lower when compared to the United States. This piece is written from the perspective of a CEO.

Our third editorial discusses and reviews in depth the Legislation and background into the US-VISIT Program. This has been implemented by the US Federal Government, in which foreign visitors coming into or out of the United States are Verified and Identified by the Biometric information and data they are required to submit, as part of the Visa Application Process. Although in theory this was designed to help protect the United States, but in reality, it has been plagued with many problems and controversies. We provide an insight into these various controversies.

The Biometric Bits Section

“An Introduction To Biometrics-Part II”

This piece is divided into the following sections:

- 1) A review of the biometric technologies available;
- 2) The differences between behavioural and physical biometrics;
- 3) A review of the major biometric concepts.

A Brief Review From Last Quarter’s Newsletter

In our last newsletter (3rd Quarter, 2009), we started an introduction to Biometrics, as well as a review of some of the major Biometric Technologies which are available today. Specifically, a definition of Biometrics was provided, and Fingerprint Recognition, Hand Geometry Recognition, Facial Recognition, Iris and Retinal Recognition, and Voice Recognition were all covered.

We continue with our introduction to Biometrics in this Quarter’s Newsletter.

A Review Of The Biometric Technologies Available

Keystroke Recognition

Keystroke recognition works by examining the unique way in which an individual types on a computer keyboard. Variables include typing speed, the length of time that keys are held down, and the time taken between consecutive keystrokes.

Signature Recognition

Signature recognition examines the way and manner in which we sign our name. Unique characteristics include changes in timing, pressure and speed during the signing process. It is important to note that it is not the signature itself that is examined.

The Differences Between Behavioural and Physical Biometrics

The above biometric technologies fall in two categories: behavioural biometrics and physical biometrics.

In general, behavioural biometrics can be defined as the non-biological or non-physiological features (or unique identifiers) as captured by a biometric system. As behavioural biometrics also covers any mannerisms or behaviour displayed by an individual, this category includes signature as well as keystroke recognition.

Physical biometrics may be defined as the biological and physiological features (or unique identifiers) as captured by a biometric system. This category includes fingerprint recognition, hand geometry recognition, facial recognition, iris and retinal recognition, and voice recognition.

A Review Of The Major Biometric Concepts

Verification And Identification

The verification process aims to establish someone's claimed identity. When you first enrol into a biometric system, it assigns you a number, which is linked to your biometric template. The database containing your template is searched on the basis of this number. If a positive match is established, you will be extended a given service or privilege. As the number is linked to the template, a one-to-one (or 1:1) relationship is said to exist.

As its name suggests, the identification process looks to establish someone's identity. In the absence of a unique number, the entire database needs to be searched in order for the system to 'recognise' you.

As the template can belong to anyone in the database, a one-to-many (1:n) relationship is said to exist.

A good example of a 1:n database is AFIS (Automated Fingerprint Identification Services), which is used by many law enforcement agencies to identify and track known criminals.

Biometric Templates

When you first enrol in a biometric system, it takes numerous images/recordings of your biological and non-biological data (including, for example, a voice recording or keystroke pattern). These raw images

and recordings are subsequently consolidated into one main image, known as the 'biometric sample'. It is from this sample that the unique features (discussed above) are captured and extracted. Next, they are converted to a 'biometric template', which, in turn, is used for the purposes of verification and identification.

It should be noted that the biometric system does not contain actual images of the biological or non-biological data - it only stores the mathematical files. The type of mathematical file that is created depends on the biometric system in use. Whereas fingerprint recognition and hand geometry recognition systems create binary mathematical files, iris recognition systems generate hexadecimal files. In other words, the image of your fingerprint or hand becomes a series of 0s and 1s (00010101000011111111, for example).

What Does This Mean To You???

As a business owner, it is very important that you have some understanding of these concepts and principles reviewed. It is one thing to say, "Hey, let's implement this, this sure sounds like a great new security system", and another thing to say, "Hey this is a great way fortify our business, but how do we evaluate this in comparison with other security systems?"

In other words, in today's economy, comparison shopping, is going to become very critical, with very tight budgets. Obviously, you can go online and do a Google Search for various Biometric Vendors, who will implement a system for you, but be sure, they will charge you exorbitant consulting fees by telling you *what **you** need* rather than ***you telling** them* what is required. So, why not save some valuable money by trying to have some understanding of key principles now, to help you understand much better what you really need???

Also, as you come closer to implementing a Biometric System at your place of business, it will be very important to include your network administrator (or whomever you depend upon to make your IT System run smoothly) in the purchase decision. Ultimately, that will be the person you will be relying

upon, especially when it comes time to exploring the various Verification vs. Identification scenarios at your place of business. For example, this person will also be responsible for establishing the various threshold settings in the Biometric System for these type of scenarios -and the type of threshold or setting chosen can have a great impact upon the effectiveness your newly implemented Biometric System.

Probably one of the biggest questions your employees will ask you will be about the Biometric Templates. The two questions you will most likely be asked are: 1) What is a Biometric Template???.; and 2) Where is the image of my hand or fingerprint stored at???. While you do not need to know the exact scientific and technical nature of what a Biometric Template is, it is important you know enough to answer your employee's questions. Ultimately, it is you the business owner, whom is responsible for acquiring this type of information and relaying it your staff and employees.

As one can see, unlike other types of Security Systems and Technologies which are present today, Biometrics is unique in that the human element (or human factors) is very much a part of it. This is a very important component which needs to be taken into consideration when you, the business owner, are considering Biometrics for your organization. The human element in Biometrics will be covered in much greater detail in future newsletters.

Editorial Section

“The Perception Of Biometrics In The United States”

Biometrics is a technology which has been around for quite a long time. In fact, the first commercial uses can be seen way back in the 1970's, with the hand geometry scanner, which is still considered to be the oldest Biometric Technology in the world, thus far.

Since then, Biometrics has seen a lot of technological advancements, with great and rapid progress being made in Research and Development. There are some very interesting Biometric Technologies which are being planned for the future, such as DNA Recognition, Gait Recognition (examining the unique features in the way we walk), and even Earlobe Recognition. These specific potential Biometric Technologies will be reviewed and discussed in much greater scope and detail in future Quarterly Newsletters.

But despite all of this, and the obvious benefits Biometrics brings to the Security Table, it still has not reached a very high level of acceptance here in the United States. Although I cannot speak for every country in the world, in comparison, the perceptions of Biometrics is very low here in the United States. There are a number of reasons for this, and they all will be discussed and reviewed separately.

Specifically, they are as follows:

- 1) The issues surrounding Privacy Rights;
- 2) Our society is very reactive and lackadaisical about Security;
- 3) The fear of the misuse of Biometric Information and Data;

- 4) The lack of Standards for Biometrics;
- 5) The fear of the National ID Card
- 6) The lack of training and support for Biometrics;
- 7) The perceived costs and expenses associated with Biometrics

The Issues Surrounding Privacy Rights

This country was founded primarily upon Civil Liberties, especially protecting our own rights as citizens. We live in the freest country in the world, and we can do pretty much whatever we please as long as it is in the bounds of the law and does not intrude upon the Civil Rights of others whom live in our society. As a result, we truly our cherish the rights to our own privacy.

Biometrics is a security tool which examines and extracts the unique features of our physiological and biological being. In fact, no other security tool does this. So, in a way, Biometrics can be considered to be an intrusive tool-it is invading our own body, and as citizens, we have no control over the Biometric Information and Data which is being collected and analyzed.

The Privacy Rights concerns has a lot of other specific sub issues surrounding it, but it is the invasion of our own physiological structure and being, as well as the total loss of control of not knowing where the Information and Data is being stored which is at the heart of the issue.

Our Society Is Very Reactive and Lackadaisical About Security

We all remember the horrible day of September 11, 2001. I for one will never forget it, and in fact I was supposed to travel that day-of all ironies-to a Biometrics Conference in Washington, DC. As we gathered the intelligence and information surrounding the detail and background of the terrorists involved, we learned the horrifying facts of the truth that in reality, this tragedy could have very well been avoided.

For example, we learned of the erratic behaviors the terrorists exhibited at the schools from which they took flying lessons, to the very poor security at the airports which could have caught them. Only after did these tragic events occur, did we, as a country come together and became much more proactive about security, as well as utilizing the various technologies which were available at the time to help fortify it.

The same can be said about Biometrics. As a society here in the United States, we have not been proactive in learning about the Security Tools which are available to protect us. If we have been more security proactive as a society, we would obviously be much more informed about Biometrics, thus increasing our levels of acceptance of it, like the other Security Technologies.

Immediately after September 11th, 2001, Biometrics was all the craze, then after awhile, it died out, and the levels of the interest or awareness about Biometrics has never really been that high with the public. My point is: Why wait for something bad to happen in order to become aware of what is available to help protect us??? Why can't we be proactive now and keep an open mind and accepting to what is out there-specifically, Biometrics???

The Fear Of The Misuse Of Biometric Information and Data

Whenever we disclose personal information, such as our phone number, e-mail address, or even our regular postal address, the biggest fear strikes us: Will this private information be acquired by a third party and misused in any way???

Well, have various protective mechanisms in place, such as the No Call List, pretty good spam filters in our e-mail systems, and even the credit card agencies are taking a much more proactive stance in protecting their respective cardholders. However, our biggest fear with the misuse of our personal information by third parties is the thought of Identity Theft, especially when we have to submit our

Social Security numbers or other types of financial data, such as our Credit Card number and its associated three digit security code.

It is this very fear of Identity Theft which has caused the acceptance and perception of Biometrics to be at such low levels here in the United States. This fear resides in the fact that if a Biometric Device were to be hacked into, and if for example, our Fingerprint Template was stolen, our identity would also be stolen forever as well. The underlying cause for this fear is that our Fingerprint, as well as our other Biometrics, are permanent physiological structures, and cannot be changed, unlike our Credit Card or Social Security number.

Compounded with this fear is the fact that Biometrics also a “Black Box” phenomenon associated with it. Meaning, when we present our Fingerprint to the Biometric Device, there are a lot of processes which take place and data/information storage we do not know about. So, we assume that all of this happens in a so called vacuum, and thus, anybody with criminal intent, can access and steal our Fingerprint.

However, a lot of these fears are just myths when examined from a technical standpoint, and can be cleared up by a clear line of communications from the Biometrics Vendor to their customer. For example, suppose somebody does steal your Fingerprint from a Biometric Device, there is not a lot that they can do with it. This issue has been addressed in the editorial in the last Quarterly Newsletter, entitled “What If My Fingerprint Is Stolen???”

The Lack Of Standards For Biometrics

As technology is introduced and matures throughout its product lifecycle, over the course of time, it “grows” so that it meshes well with other technologies and related platforms and applications. For example, as a new software product is introduced into the marketplace, it is tested so it can work

well with the other operating systems, in particular Windows and/or Linux. However, in order for the to mesh well with the other technologies, it is very crucial that a set of Best Practices and Interoperability Standards be created so that the differing technologies can all work together upon a common platform.

A prime example of this are the various types of networking devices (such as routers and firewalls) working together on a common Internet Protocol, such as TCP/IP. A list of Interoperability Standards has to be created in order for this unison of networking devices to actually occur. As the Biometrics Market is booming and maturing, there are many types of products coming out. For example, just this year alone, there have been a lot of technological advances made in Iris Recognition.

But, as these new Biometric Products and Solutions are coming out, there is no established list of common Interoperability Standards. It is not that Biometrics is such a new piece of technology- but rather, nobody has had the initiative to come out with such a list of Interoperability Standards. As a result, the Biometric Vendors all over the world are making all sorts of claims about their Products and solutions with no solid baseline to be compared against with. As a result, this causes confusion for the end user which basically diminishes the level of trust with the Vendors, and ultimately leading to the low perception of Biometrics here in the United States.

However, this low perception is not just with the end user or average consumer. Even the more technical people (such as software developers) , I have discovered, also have a rather low perception of Biometrics from a development standpoint. This is because of the fact once again, of the lack of Interoperability Standards between the various Biometric Vendors. Very often, software developers have a hard time developing applications which can interface with the other technologies which are available.

Even on a much more macro level, applications which require the use of Biometrics in some type of fashion are also having a hard time getting off of the ground. This is best exemplified by the National ID Card and the e-Passport. Governments around the world (such as here in the United States) are trying to implement a National ID Card with a Biometric implemented into it, such as Fingerprint scan or an Iris scan. But, because there are no Interoperability Standards, there has been a very hard time trying to get these new types of security documents off the ground.

For example, the National ID Card and the e-Passport have to work with legacy Information Technology systems worldwide in which they can be processed and accepted at points of entry and exit. This is especially true for the e-Passport, because travelers will be using this security document all over the world. So as you can see, the need for Interoperability Standards becomes even more paramount.

However, it is important to put a disclaimer here. With regards to the implementation of the National ID Card, and the e-Passport, there are many other reasons as well why they have been difficult to put into place—Biometrics has been only part of these difficulties.

The Fear Of The National ID Card

The last section mentioned the National ID Card and the e-Passport. Currently, here in the United States, there is no common, one Security document across all of the fifty states which can Identify and/or Identify an individual. Instead, each state has their own driver's license or state ID card.

There is no uniformity among these cards. Also, they can be replicated very easily. Probably about the closest thing we have to a common document is the traditional Passport. But, not all US citizens have this type of Passport, only those whom travel abroad have this document with them.

After September 11th, 2001, the movement for a National ID Card proliferated-so that there would be one standard in which to Verify and/or Identify people. The idea is that this would be an all inclusive

Security document, complete with a picture, Fingerprint, and various types of other Biometric Templates, such as a Facial Scan or an Iris Scan. However, the National ID Card has received, at best, an extremely lukewarm reception here in the United States. This is primarily because the public at large is afraid that the Federal Government will have control over our most private information which is contained in the National ID Card-in particular, our Biometric Templates.

As a result, this has led to an outcry of the violation of our Civil Liberties, and especially, our Privacy Rights being taken away. Consequently, this has also led to the poor perception of Biometrics here in the United States as well. It is important to note, that other countries around the world, have been successful, or have been trying to implement some sort of a National ID Card Infrastructure. To the best of my knowledge, the citizens of these various countries have been much more receptive and open to the thought of a National ID Card in their respective country.

There are probably numerous reasons why people in other parts of the world are much more receptive to a National ID Card than people here in the United States. Probably the fear of Privacy Rights is much less, there is more open mindedness, etc. But, a key reason could be is that people in these countries are much more informed about Biometrics-and as a result, they are more proactive about their Security practices.

Also, it could very well be the case also that the Governments in these countries are conveying a much clearer message about how Biometrics will be used on their citizens, **and this is a key, fundamental Human Factors about Biometrics-conveying how the information/data will be used, and for what purposes.**

The Lack Of Training And Support For Biometrics

Whenever we are introduced to a new piece of technology, especially in the workplace, there is often

some sort of training, workshop, or just a tutorial to get you acquainted with the new software. You may now embrace the new technology you now have to work with, but with the training you have received from your employer, you are probably at least willing to accept it, work with it, and make the best of it. Most technology vendors are aware and recognize this fact of the need of training their end users. After all, this is a huge factor in the acceptance of their products.

However, most Biometric Vendors still do not seem to understand this simple fact of the need to train and educate their customers and end users. This appears to be a very common trend today, both across the large and small Biometric Vendors. The sad truth of the matter is that Biometric Vendors simply sell or just install the Biometric Device for their customer. But, they very often do not train them, or even offer advice in how to use their product or solution.

As a result, the end user or customer is left very frustrated, and has developed a defeatist attitude towards the Biometric Device-because they are poorly trained in how to use it right the first time. Thus, this also contributes to the low perception of Biometrics-based simply upon the fact of the lack of understanding and the lack of training. To make matters even worse, with most of the technology tools available on the Internet, an end user can look information via a simple Google search. However, this is not even the case with Biometric Technology. There is even concern amongst the Federal Government of the lack of training, especially with the Department of Homeland Security.

There are also so called Biometric Consulting Companies out there in the marketplace, and the main line of their business is to provide consulting services to their clients whom are interested in implementing Biometrics at their place of business or organization, and are in the decision making phase of what they will need and what to get. Very often, on the part of the Biometric Consulting Company, fancy buzzwords and techno jargon is used, but once again, there seems to be the fundamental lack of understanding here as well about the lack of educating the customer about Biometrics. For instance,

the customer not only needs to understand about what Biometric Device they will need to acquire, but they **also need to understand and be educated about the Perceived Benefits and the Perceived Ease of Use of the particular piece of Biometric Technology they are interested in.** These two factors, Perceived Benefits and Perceived Ease of Use are also very important components in the overall equation of the perception of Biometrics.

Yes, it sounds very easy to simply say that in order to help increase the acceptance of Biometrics, all a Biometrics Vendor has to do is to provide training to their end user-However, unfortunately, in the real world, things are a lot more complicated than that. For example, in a training program, there is a very fine line to be drawn between just talking about the techno-jargon associated with Biometrics and actually explaining to a level that the end user can understand in a very short time without getting frustrated. Future Quarterly Newsletters will discuss what needs to be specifically addressed in a training session.

The Perceived Costs And Expenses Associated With Biometrics

When one thinks of a Biometric Device, the image of something very high techy, and James Bondish always gets conjured up. With these mental images, also comes the perceptions and notions of fancy gizmos which are extremely expensive. As a result, this has also been a factor in the low perception of Biometrics-its perceived high cost and expense.

There is no doubt that Biometrics can be very expensive-but, one has to bear in mind that the more elaborate a setup is and the more sophisticated type of application it is being used for, the higher the cost, and expense. At one point in time, all Biometric Devices were very expensive, but just like computer hardware, the prices have reduced substantially. For example, today, simple Biometric Devices such as Single Sign On Solutions for your computer or network are cost anywhere between \$100-\$200, thus making them reasonably affordable. Heck, you can even buy a very rudimentary

Biometric Device at your local office supply store (such as Office Max or Office Depot) and even buy a Fingerprint Recognition Device for less than \$50. Even the once traditional expensive Biometric Devices such as Iris Recognition, have also dropped in price substantially as well, making them even more affordable.

Also, it is important to keep in mind as well that there are many more Biometric Vendors coming out into the marketplace as well. And with this crowding of people, the law of economics certainly holds true: An increase in supply leads to a decrease in price. Further, the size and portability of Biometric Devices will become much smaller, and could very well fit into your pant pocket-much like the evolution of cell phones.

However, the Biometric Vendors need to do a much better job at communicating their prices, especially to the end user. The Vendors tend to focus on the much more specialized markets rather than just the average consumer, or end user. In other words, there needs to be a much better flow of communication between the Biometric Vendors and the consumer-only then will the public be aware of the affordability of Biometric Devices.

Editorial Section

“Biometrics in Africa: The Basis For The Emergence Of The Individual”

*Written by: Gary Chalmers, CEO, iPulse
Systems(Pty), Ltd.*

As the CEO of a biometrics company for just over two years now, and a technologist for life, I have watched with fascination the growing penetration of biometrics into the African market.

It is truly a phenomenon to watch how third world counties can leapfrog first world ones through the adoption of emerging technologies at a rapid rate. This growth is driven by the fact that there is no legacy system or investment to replace, thereby removing the natural reluctance of business and government to write off undepreciated and paid for infrastructure.

It is just such an occurrence that has driven the gradual shift on this continent towards biometrics, with the next few years promising exponential growth in the adoption of these technologies in Africa.

Africa & Populations – A Brief History

Whilst Europe and the USA battle privacy laws and other such niceties, Africa sees in biometrics a way to

bring definitive identification to a continent where illiteracy is rampant, and many people do not know when they were born, nor have any record of the event available to them.

With limited resources, African countries have struggled to identify and even count their populations, with the constant movement and migration of populations, not to mention the regular, often violent changes in government, causing havoc amongst what little records exist.

A census in Africa is not the organised, mathematically correct and defensible event that European and American citizens take for granted. Rounding errors and estimations can add or remove millions from the tally, leaving countries with a population that could vary in reality from the final number by as much as 20% or more.

Alien residents in countries number in the millions, as individuals move to find family and tribe members across border lines demarcated by conquerors decades ago, and which have no bearing on where tribes lived or roamed in the past.

In addition to this, war, famine and the desire for a better life drive millions from their place of birth each year, into cities and even countries who have no idea who they are, or where they came from.

Biometrics – The cure for all

Africa is not for sissies they say. It's a tough continent, where the weather, the people and fate seem to take no mercy, and filing cabinets are in short supply. When you live in a mud hut in a rural village with no telephones or internet or connectivity, your birth is seldom marked by anything other than the phase of the moon or the season, tied back to the year of the great flood, or big fire. These types of markers do not make for an accurate national identity system.

In the past few years, and in line with the adoption of technologies mentioned earlier in this article, the emergence of the mobile phone, and the rampant growth of these networks, has finally made instant and reliable communication a reality in Africa.

The past two decades have been the Era of Connectivity in Africa, with the coming decade showing signs of being the Era of the Individual – making individual people count on a continent that has low value for life.

Biometrics has a key role to play in this renaissance. Throughout Africa, governments are moving towards national identity programs that will allow their populations access to services such as education and healthcare, and which will logically increase the value of life.

Companies such as ours, steeped in the culture of this continent, and understanding the desire and need of our sister countrymen, are building solutions that are customised to this harsh environment, and which take into account the primal needs over the simple niceties of the first world.

In Maslow's hierarchy, self actualisation is the pinnacle, not the base, and biometrics answer a fundamental need for populations that transcend such issues as privacy laws and inconvenience.

The ability of an individual to be identified by no more than the combination of their name, photograph and fingerprint, all of which are easily portable and do not require documentation, is a panacea for the governments of Africa.

It is my firm belief that the continued growth and rise of this continent from the dark to the light can only be achieved through the individualisation of the inhabitants, and that given the challenges that face

us, this can only be achieved through the creation of national identity systems which take into account the lack of erudition of these individuals.

Knowing who you are, and that you matter as an individual, is the first step towards true freedom, and ultimately, self actualisation. Biometric technologies will be at the heart of this revolution, and are already allowing countries to achieve an accurate census of their populations, and to use these numbers to drive informed policy formulation. This in turn will allow effective health and education programme implementations, which will drive investment and natural entrepreneurial growth in the economy.

About The Author: Gary Chalmers

40 years old, born in Johannesburg, South Africa, Gary was the founder of Training Connection, a company specialising in technical training, specifically in the Microsoft field. In October 1997, Gary sold his share of Training Connection into the holding company Connection Group, and accepted a contract to become the International Marketing and Sales Director for CompTIA USA. Completing this 8-month contract, Gary returned to South Africa, bought back Training Connection, re-launched as Torque-IT, and was involved in running the company until his resignation in 2007, when he joined the Richmark Group to serve as CEO of iPulse Systems.

Gary has an excellent overall knowledge of the ICT market both locally and abroad, and an extensive technical background across a broad field of topics.



Editorial Section

“The US-VISIT Program And Its Controversies”

Abstract

When thinking about Biometric Technology, one always wonders how it is used—in the Quarterly Newsletters thus far, I have discussed in varying lengths two major market applications of Biometrics: Physical Access Entry and Single Sign On Solutions. These are fancy names, but the former merely refers to the fact that you can use your hand, eye, or finger to open a door, and with the latter, you can use or eye or fingerprint to log into your computer, essentially replacing the need to remember hundreds of passwords.

But, the above are just two of the primary market applications-Biometrics is also being used in a wide variety of other areas, such as E-Commerce, Security Documents, Welfare Programs, Smart Cards (these are just like credit cards, but instead, they contain a memory chip in them which can hold a lot of Security Information in them, such as Biometrics), and yes, even the Federal Government. Because in large part because of this Global Recession, there has been a downturn in the private sector of the purchase and acquisition of various types of Biometric Solutions, and as a result, there has been an upward shift by the Federal Government for the purchase and acquisition of these Biometric Solutions.

In fact, right now, it is the Federal Government which is the biggest player in the Biometrics marketplace. Biometrics is being used in a lot of the facets of the Federal Government Operations, including Legislation which has passed or is still pending, in the name of protecting US Citizens and the nation as a whole. The two biggest users in the Federal Government are the Department of Defense (primarily because of the simultaneous military engagements in Afghanistan and Iraq), and the

Department of Homeland Security.

With regards to the Federal Legislations which are passed or still pending, there are always issues, concerns, advantages and disadvantages voiced by the politicians, Corporate America, and the American Citizens.

In this Quarterly Newsletter as well as each and every future issue, there will be an Editorial Section which discusses the role Biometrics plays in Federal Legislation, and the issues/concerns which impacts the everyday American Citizen, as well as people around the world. In this Quarterly Newsletter, we provide an introduction and background into a piece of Federal Legislation known as "US-VISIT".

This essentially mandates and uses Biometrics to Verify and/or Identify individuals as they enter and exit the United States, as well as other major points of entry and exit dispersed across the US.

The US-VISIT Program has certainly created its fair share of controversy and criticisms, which will also be examined.

The US-VISIT Program: It's Origination

The origination and thinking of the US-VISIT Program actually started in the mid 90's, at the time of the Internet Boom. During this period, the Congress of the United States had asked the Attorney General to come up with a method which would collect and store the departure and arrival information of each and every foreign visitor entering into the United States. However, the basic premise was to get away from a cumbersome, paper based system of keeping track of the entry and exit information and data of every foreign visitor entering into the United States, and instead, implement a system which would do all of this automatically.

This piece of Legislation became known as "Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996", or "IIRIRA" for short. Eventually, this piece of Legislation was replaced with a newer piece of Legislation which came to be known as the "Immigration and Naturalization Service Data Management Improvement Act of 2000", or simply known as "DMIA" for short. The differentiating factor with these two pieces of Federal Legislations is that the latter called for the key integration of the existing databases between the Department of State and the Department of Justice, which kept track of the arrival and departure information of all of the foreign visitors to the United States. Thus, this gave birth to the US-VISIT Program.

Just immediately after the tragic events of September 11, 2001, two new pieces of Federal Legislation were passed which became known as the "Uniting and Strengthening of America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001", and the "Enhanced Border Security and Visa Entry Reform Act", which are also called the "USA Patriot Act" and the "ESA" for short, respectively.

The USA Patriot Act imposed speed into the automated system of keeping track of the entry and exit of the foreign visitors, and it also mandated that the newly created Department of Homeland Security

also be a key partner in this automated process. Also, for the first time, the USA Patriot Act called upon the use of a certain piece of Security Technology which would set the benchmark for this automated system-this piece of technology is known as Biometrics.

The ESA broadened the powers of the USA Patriot Act and the other mentioned pieces of Federal Legislation by setting up much more ambitious goals and benchmarks, which are as follows:

- 1) The creation and implementation of a database which would record the arrival/exit data for each and every foreign visitor to the United States from machine readable Security Documents, such as Passports, Visas, ID Cards, etc.

- 2) Biometric Information and Data would have to be included into these particular pieces of Security Documents;

- 3) All of the Information and Data contained in these Security Documents would have to possess the ability to be transmitted electronically by all types and kinds of Foreign Carriers;

- 4) All of this Information and Data must be made accessible and presentable upon demand to any law enforcement official whom are responsible for “the investigation and identification of aliens”.

With all of these pieces of Federal Legislations and strategic benchmarks, the US-VISIT Program is what it is today, created by a lightning rush fueled with a sense of urgency, in protecting and safeguarding the United States.

The US-VISIT Program: The Structure Today

At the present time, the US-VISIT Program is completely a 100% inkless effort, since Biometric Technologies are now employed. With the current system, any foreign visitor wishing to come into the United States has to go through the normal US Visa/Passport issuance process at the US Embassy, of country of embarkation/departure. But now, in addition to this, the foreign visitor has to submit both index fingerprint into a Biometric System, as well as have a digital photograph taken.

Upon entry/disembarkation into the United States, the Customs/Border Protection Officers then compare the index fingerprints Biometric Templates in the US-VISIT Database with the other travel documents held in possession by the foreign visitor. Although this process may appear to be very simple, the US-VISIT System must integrate with many other databases kept by the Federal Government, not only because of the Legislations which have mandated this mammoth integration, but also because there are so many foreign visitors entering and exiting the United States every day, the US VISIT System may not be able to capture all of the entry/exit information just by itself.

The following are examples of some of the other Federal Government databases the US VISIT System must integrate with:

- 1) *The Arrival Departure Information Database (also known as "ADIS")*: This records the foreign visitor arrival and departure information.
- 2) *The Advanced Passenger Information Database (also known as "APIS")*: This also contains arrival and departure information of foreign visitors, but this is passenger manifest information.
- 3) *The Computer Linked Application Information Management System 3 Database (also known as "CLAIMS 3")*: This contains the information and data of foreign visitors whom are requesting benefits from the Federal Government
- 4) *The Interagency Border Inspection System Database (also known as "IBIS")*: This contains information and data on potential suspects (based upon "lookout data").
- 5) *The Automated Biometric Identification System Database (also known as "IDENT")*: This also contains Biometric information and data on foreign visitors.

6) *The Student Exchange Visitor Information System Database (also known as "SEVIS")*: This holds Information and data exclusively about foreign students in the United States.

7) *The Consular Consolidated Database (also known as "CCD")*: This stores information and data about foreign visitors who have applied and not applied for a visa, and if they possess a visa, if it is valid or not.

Through the integration of all of the above mentioned databases and even more databases not mentioned, the following are the specific types of information and data which are extracted by the US-VISIT System on foreign visitors:

- 1) The name of the foreign visitor;
- 2) The date of birth of the foreign visitor;
- 3) The country of citizenship of the foreign visitor;
- 4) The gender of the foreign visitor;
- 5) The appropriate passport number of the foreign visitor, and the country where it was issued;
- 6) The country of residence of the foreign visitor;
- 7) The visa number, the date of issuance, and the place of issuance of the visa the foreign visitor possesses;
- 8) The address of the foreign visitor of where they are staying at in the United States.

Initially, when the US VISIT Program was started, it was meant for those foreign visitors coming from countries in which the United States required a visa. At this point in time, countries which were in the Visa Waiver Program were not required to be part of the US VISIT Program. But however, on September 30, 2004, the US VISIT Program was further broadened and enhanced (via its Legislation) to include those countries which participated in the Visa Waiver Program. This meant that those foreign visitors whom were staying for less than 90 days in the United States and did not require a Visa were now faced with a much stricter set of rules to follow, as well as increased Security measures. These

countries included mostly all of the European countries, as well as Andorra, Brunei, Japan, Morocco, New Zealand, San Marino, Slovenia, and Singapore.

Also, the enhanced USA Patriot Act Legislation also required that these countries which were once in the Visa Waiver Program also had to implement machine readable passports which would have Biometrics incorporated into them, and that these new types of Security documents also had to comply with the standards established and set forth by the International Civil Aviation Organization. Because of these enhancements to the USA Patriot Act, the US VISIT Program is deemed to be the largest Biometric based system in the world, by sheer virtue of the fact of the large volume and numbers of foreign visitors entering and exiting the United States on a daily basis.

The US-VISIT Program: The Numbers and The Statistics

Finding the exact statistics on the US VISIT Program is not easy, but the following numbers are the most recent statistical trends and data as of Fiscal Year 2007:

- A grand total of 46,298,869 entries by foreign visitors into the United States was recorded.

Within this grouping:

- 236,857 foreign visitors were identified as possibly overstaying their Visa;
- There were 237 arrests made by the Immigration and Customs Enforcement officials;
- 25,552 database hits resulted in the adjudicating process of Visa applications of foreign visitors;
- 11,685 Biometric database hits at the major points of entry into the United States, some of these were people with a criminal past;
- 31,324 database hits were used to closely scrutinize those foreign visitors applying for United States Immigration benefits.

There has also been an increasing trend for the Federal Government funding of the US VISIT Program:

- Fiscal Year 2004: \$330 Million
- Fiscal Year 2005: \$340 Million
- Fiscal Year 2006: \$340 Million
- Fiscal Year 2007: \$362 Million

It should be noted that in the face of increased Federal Government funding, the US VISIT Program, while according to what the term “successful” really means, has yielded in arrests and tracking down illegal immigrants whom are criminals, but has not directly caught any hardcore terrorists per se.

The US-VISIT Program: The Controversies

As in with all types of Federal Legislation and Mandates, there are always the critics, the criticisms, and controversies depending upon the magnitude and the type of Legislation passed. Since the US-VISIT Program is global in nature, it certainly has received and continues to receive its fair share of the controversy pie. And not surprisingly enough, it is the use of Biometrics, either directly or indirectly, which is causing the major stir.

Remember, as written previously, the US-VISIT Program had its origination and roots back in the mid 90's, and while the concept of it at that point in time appeared to be well received and well intentioned, it was passed in a sheer haste and in a haphazard fashion right after September 11th, 2001, with the side effects, namely its controversies, being felt today.

This section of the Quarterly Newsletter will present and outline the issues and controversies surrounding the US-VISIT Program, but the next Quarterly Newsletter will actually review them in much more detail and scope.

The Issues

1) As written previously, there is increased Federal Government spending, year after year, for the US-VISIT Program. While there have been arrests made and Visa applications are being much more closely scrutinized, there have been no hardcore terrorists or suspects caught, despite the heavy investments being made, especially in the Biometric Technologies and the integration of the Federal Government databases. As a result, there is a general feeling that Security has not been increased, and that the United States is just as vulnerable as before.

2) The US-VISIT System makes use of and integrates with a wide array of databases across the Federal Government. Although it has been promised that the use of the information and data, as well as the Biometrics which are collected into them will be used only for lawful and necessary purposes, this has only been spoken of in broad terms and not in exact, specific terms. For example, the

specific powers of the Attorney General have not been spelled out in this regard. Thus, there is great fear in that the information and data, especially the Biometrics component of it, will be misused.

3) Since the US-VISIT Program has had its Legislation further magnified by requiring that virtually all foreign visitors (including those whom are eligible for the Visa Waiver Program) must submit their Biometrics and be digitally photographed, other countries have become “upset” about this, and in reciprocity, have implemented their own version of the US-VISIT Program, especially targeting United States citizens, whom would not have normally been required before to submit their Biometric information and data. These countries include Brazil (they implemented their own program in January of 2004); Japan (their system was implemented in November of 2007); and South Korea (they will implement their own program in 2010).

4) Initially, the US-VISIT Program required that only two sets of Biometric Templates (one from each index finger) be submitted by foreign visitors. But because of the increased Legislation, the US-VISIT Program now requires Biometric Templates from all of the fingers (this results in a set of ten Biometric Templates) of each and every foreign visitor.

5) According to a GAO (Government Accountability Office) Report, the Information Technology system of the US-VISIT Program is full of Security weaknesses and flaws, especially in the way the Biometric information and data of all of the foreign visitors is being held and processed.

6) On a topic related to Biometrics, at one point in time, the use of Radio Frequency Identification (RFID) was given consideration to be implemented into the US-VISIT Program as a Security Add-On. Numerous tests were conducted, but they failed, and as a result, the Department of Homeland Security dropped all together the plans to use RFID. Numerous reasons were cited for this, especially the lack of Security and Privacy safeguards, and the fact that the RFID Technology could not Verify/Identify the same foreign visitors leaving the United States as the same ones who entered the United States.

7) One of the biggest criticisms of the US-VISIT Program has been its lack of concern and even possible violations of Privacy Rights with regards to the Biometric information and data collected from the foreign visitors as they enter into the United States. A few examples of these are the lack of timeliness for the completion of a Privacy Impact Assessment for the US-VISIT Program (this is required by the E-Government Act of 2002). Also, the US-VISIT Program has a Privacy Rights Officer whose “duty is to ensure that the privacy of all visitors is respected and to respond to individual concerns which may be raised about the collection of the requested information”. But, the point of contention has been that the Privacy Officer has too much of discretionary powers to respond to complaints set forth by foreign visitors, and has not been quantified. As a result, there is no clear cut legal or judicial path of recourse for the foreign visitor if they are denied entry into the United States, because of the US-VISIT Program. Also, there is a very obscure path for the foreign visitor if they want to correct or update any misinformation about their Biometric information and data. Finally, the Department of Homeland Security, it appears, is not under any sort of legal obligation to keep the Biometric information and data up to date and accurate.

8) Apparently, while most other countries around the world are required to participate in the US-VISIT Program, Canada and Mexico are not, subject to certain rules. The rules with Mexico are that if a Mexican citizen travels into the United States with a Border Crossing Card, and if they stay more than 72 hours in the US, they are then subject to US-VISIT, and have to submit Biometric information and data. With Canada, the Biometric information and data is only collected from Canadian citizens if they come to the United States for a brief visit, and do not wish to pursue an Immigrant Visa. This imbalance of being less stringent with Mexico and Canada (especially because the United States and Canada have the longest stretch of poorly protected border in the world) has created controversy, with Those countries which are required to participate in the US-VISIT Program, no matter what.

The US-VISIT Program: A Summary

The controversies are just some of the problems the US-VISIT Program faces. Obviously, there are much more, and future Quarterly Newsletters will examine them in much further detail. The goal this Quarterly Newsletter was to present a survey of some of these problems.

Right now, it is believed that the US-VISIT Program is the largest Biometric program in the world ever undertaken by the Federal Government, more so than the National ID Card, the e-Passport, etc.

As Biometrics becomes more prevalent in the Federal Government sector, this will obviously have a big impact on the US-VISIT Program, as well as its future uses.

We will stay on top of this, and provide updates via the Quarterly Newsletters and our Blog Site (biometricnews.typepad.com).