OPINION

# Guilty Until Proven Innocent

**Divya Titus**
*Candidate for M.Sc. in Analysis Design and Management of Information Systems*
*Information Systems and Innovation Group*
*Department of Management*
*London School of Economics*

Often and quite appropriately dubbed as Big Brother, Biometric technology is finally taking off the shelves. Biometric technology involves recognizing humans based upon specific behavioral or physical traits. It recognizes these unique characteristics and then uses them to verify the individual's identity. Primary biometric disciplines include fingerprinting, facial recognition, voice recognition, iris recognition, palm scan, retina scan, hand geometry, signature-scan, keystroke scan and body movements. Fingerprinting is the largest segment accounting for almost fifty percent of biometric technology.

**Why Biometric Technology?**

Recent tragedies such as 9/11 (the 11th September, 2001, terrorist attacks in the United States) and more recently 7th of July (the London terrorist bombings) attacks have magnified the necessity for higher security standards. Aftermath 9/11, the United States government has become a strong proponent of utilizing biometric technology to address rising security concerns especially in areas such as visas, immigration, and government identification cards. Other governments of countries such as Australia, Germany, Israel, etc. have followed suit and have made significant investments in border and passport security projects. Common identification methods involve identification card, personal identification numbers, passwords etc. The keen interest in biometrics stems from the fact that it is so closely bound to a person i.e. unique .The likelihood of it being lost, stolen or falsified is considerably lower.

The hype that surrounds the use of biometrics for security measures is nearly a decade old. It was often believed to be a technology propagated and driven by governments, and thus confronted with concern from the general population who viewed it as an infringement on their privacy. For instance, biometric authentication uses personal data that is intrinsically linked to the individual and hence is a favorable medium of security within public domain applications. Such applications involve both governments and common citizens. While the government owns the technology, the citizen finds him or herself targeted by it! This is bound to create a rather delicate situation where the applications are often scrutinized as well as highly accountable for both the government security and that of the public. Biometric data are so personal to an individual, making security of this data a primary issue. While the biometric system itself needs to be secured, the users must also be protected from the possible divulgence of their personal data to third parties. Such public domain applications are spread over the globe which results in sensitive data (biometric or other personal data) being transmitted over the internet or across other unprotected communication links. Illegal acquisition of this data will pose serious threats to operational security.

Post 9/11, severe security measures were implemented within the USA's 115 international airports and 14 major seaports. All international travelers belonging to the visa waiver program (VWP) countries (Australia, Sweden , Germany, France etc. ) now require machine readable passports that consist of biometric data (an e-Passport) if they wish to travel without a visa on the VWP. While air travel has become more complex and tedious upon introduction of additional security checks, the public is now reassured of the drastic measures taken by the government to protect them from terrorist activities. Another area of biometric usage by governments is that of e-Borders. This relates to the use of IT and security measures for modernized border control. Biometrics for passengers upon entry into the country, are collected and then used for surveillance and profiling of passengers. The USA launched project US-VISIT in which customer profiling begins overseas in the US consular offices. While issuing visas, biometric information such as digital fingerscans and photographs are checked against a database of known criminals. Upon entry into the USA, the fingerscans are verified to ensure that the same person who was issued the visa is now entering the country. The UK followed suit with project Semaphore to facilitate cross border information sharing. Information of such mammoth proportions may cause more and more people to be turned away at the border. In the case of Yusuf Islam (former singer Cat Stevens) was deported to London from the United Stated when his name popped up on the no-fly list. In an interview on Larry King Live (7th October, 2004), Yusuf Islam mentioned that the border officials confused him with a man on the no-fly list named "Youssef Islam". While biometric technology may ensure prompt security clearance of low risk passengers there are bound to be many more innocent passengers that are unjustly denied entry! Both projects have received much flak from privacy groups and human rights groups. Fingerprinting all visitors to the USA is viewed as criminalization of non-Americans. Meanwhile the US government gaining access to airline reservation databases was opposed by airlines, NGOs, and the European Commission based on costs, civil liberties, and privacy respectively.

Another outcome of the biometrics – government association has been the National Identity Card saga in the UK. Biometric ID cards contain biometric information such as facial recognition, iris scans and digital fingerprints and various other personal details all on a single card. If the government were to have its way, all this information would be stored on a central database that is easily accessible to the government, police, immigration, inland revenue service and national intelligence services. This move has been widely criticized, most vehemently by the London School of Economics. Professor Angell from the department of Information Systems at the LSE perceives this to be the last of the big government IT projects as he claims it will result in "diabolical shambles". Simon Davies (visiting professor, LSE) slams the project on the basis of high implementation costs which will eventually be borne by the tax payer. Others view the compulsory Na-

tional Identity Card as a compromise of the British tradition, civil liberties and privacy. Meanwhile the British government, led by Prime Minister Tony Blair, has maintained this as an issue of "modernity" rather than civil liberties in order to track issues such as identity fraud and terrorism. The questions we are left with are:

*Are National Identity cards just another document for miscreants to forge?*

In May 2003, the International Civil Aviation Organization (ICAO) approved facial recognition as the global standard of biometric data. Image recognition has never been a human's greatest asset and hence it is less so for machines. The expected error percentage may vary between 5% and as high as 40%. Professor John Daugman (Cambridge) describes the performance of the computer algorithms for face recognition as "appalling" in terms of accuracy. The slightest variation in facial expressions, pose angle, or the viewing angle may have detrimental effects on the accuracy of the computer algorithm.

**Are all citizens guilty until proven innocent?**

Professor Daugman mentions the key strength of biometrics in being able to recognize individuals based on the degree of randomness and complexity that biometrics contains. This explains the unreliability of face recognition where the degree of randomness is far lower than that present in fingerprints or iris scans. The iris is associated with almost 249 degrees of freedom as compared to the 20 degrees of freedom of the face. The one thing that is certain is that every technology brings with it a degree of uncertainty. No biometric can offer 100% accuracy. There will always be a margin of error. All biometric data collected will be stored in databases. But in order to match this data against criminals or terrorists, the terrorists must at first be registered within the database as terrorists! While there are a certain number of known terrorists, it is likely that a majority of them haven't been discovered yet.

Easily inferred, major obstacles to public acceptance of biometrics are security and privacy-related issues. Information technology provides features such as Public Key Cryptography to enhance security but there is also a human factor involved: certain staff will have access to the biometric databases and hence it is absolutely essential that they are trustworthy. Illegitimate changes to the database or incorrect changes will have drastic effects. Other methods of security are periodic security audits and liveness checks which attempt to detect features such as response to stimuli (light, electrical pulse), thermal measurement, moisture etc. This makes one question the advancement of technology, does technology cater to external causes that may influence our response to stimuli. E.g. will our reaction to light or electrical pulse be same under influence of alcohol or drugs? Are machines intelligent enough to detect the difference?

**Biometric security - boon or a bane?**

Biometric technology uses a 'two factor' authentication: it relies not just on something we know (PIN or password) but also on something we possess. Therein lies the allure of this technology: it is believed to be a technique to combat online crime or identity theft. Voice verification systems are being adopted for telephone banking procedures within the banking industry. Laptops are beginning to be equipped with fingerprint readers. Biometrics is also used for safety locks in safes, houses, garages etc. Following the success of the i-Mode in Japan, m-commerce has taken a huge leap worldwide. Users can access websites, send e-mails, mobilize funds between banks and even shop online using their mobiles. The Achilles heel in this case is the mobile application. SecureTest (security consultancy) demonstrated the security perils of such applications where hackers can tap into the mobile phone application, modify the code, and ultimately manipulate the website itself. This is witness to the fact that the improbable has now turned possible! Biometrics such as fingerprint readers are now being used to secure mobile transactions. In an era where mobile phones are synonymous with monetary transactions securing one's handset is of primary concern.

Biometrics may enhance security but a major impediment to a biometric is that once it is compromised, it has been compromised for life! Unlike other modes of security such as passwords, PINs, etc., which can be changed periodically, a biometric is unchangeable. Stolen biometrics can lead to catastrophic outcomes because biometric features such as fingerprints are not easily changeable and hence may plague the victims for decades. There is always a threat of biometric information being grazed and used to identify people which may then lead to criminal acts such as kidnappings. In Malaysia (2005), four armed gangsters attacked an accountant in the suburbs of Kuala Lumpur in order to steal his Mercedes S- Class. But upon acquisition of the car they realized the car was operated by a fingerprint recognition system. So they stole the car and left the victim stripped naked on the road, but not before they cut off the tip of his index finger incase they needed to disarm his immobilizer at another time. In 2006, popular television show *Mythbusters* attempted to break into a laptop and security door armed with biometric authentication. Trespassing the laptop proved slightly more arduous but the security door was opened 3 times using 3 different techniques in less than 10 minutes! The security door was armed with a fingerprint reader which also measured pulse, sweat and temperature (i.e. live sensing). A licked latex copy of the fingerprint was all it took to dupe the machine. This does pose a startling question:

*Are biometrics as reliable as a strong form of authentification?*

While there have been considerable legal, security and policy implications, there have also been cultural and social issues related to the implementation of biometric technology. There is a perception that with the introduction of biometric technology our society will soon transform itself into a surveillance society. Fingerprinting children at UK schools was not received kindly by social groups and parents. While the Department of Education and Skills maintains that this biometric information is only used to make school services such as libraries and canteens function more efficiently, the parents and other social groups believe this is conditioning students to develop a casual attitude towards biometric information which in turn will lead to increased identity thefts.

For every biometric there will be a certain group of people who are physiologically unable to use the technique, for example, an arthritis patient is unable to place his/her finger flat on a fingerprint reader. Sometimes there are apprehensions associated with the use of certain technologies: the initial retina scan was often feared because people were intimidated by the proximity of machines to their eyeballs. Other factors and issues that may deter the acceptance of biometric technology

are those of hygiene: there may be general discomfort while using fingerprint scanners or placing one's face against a machine during a retina scan that we know to have been used by numerous people before us. There may also be certain religious reservations, because in some religions imagery is forbidden.

Earlier market predictions often expected the government and financial sectors to lead the biometric markets in annual revenues. However, recently there has been an upsurge in the usage of biometrics for commercial purposes. Owing to a low product demand as a consequence of government expenditure, a number of vendors are now exploring the commercial possibilities of biometrics. A very common commercial use is that of finger scans or palm scans at supermarkets used in tandem with a PIN, which eliminates the use of credit and debit cards and also results in shorter queues. The fingerprint and the PIN are then searched against a central database before the transaction is authorized. While this is rather convenient, it seems less secure. But it is argued that this level of security is more than adequate while shopping where the scanner is constantly monitored by a shop employee and hence any suspicious action will be recognized almost instantly.

An interesting observation is the response of the general public. While the usage of biometric technology by the government has been constantly opposed and looked at with suspicion, the commercial use of this technology has shown a steep increase. The largest commercial application of biometrics within the United States is Disneyland, where, in order to combat ticket fraud, they have been constantly recoding the geometry and shape of fingers into the ticket as opposed to photo identification which is more time-consuming. Following a technology upgrade, they now use a more sophisticated scanner which scans a single finger to obtain relevant biometric information. This has further reduced customer wait times. It comes as no surprise that post - 9 / 11 the US government requested Disney's advice on biometric security.

It is estimated that in USA more than 3 million people currently pay for goods using fingerprint biometrics. The only logical reason for this display of double standards is that the commercial applications of biometrics provide direct benefits and incentives to the customer. While governments battle public resistance of identity cards and e-passports, customers seem to willingly embrace commercial applications. It might be an interesting point for the government to note: on the commercial front, all it took for the biometric technology to sway customers in their favour were a few personal benefits and shorter queues.

The governments have knowingly or unknowingly cast a shadow of fear over its citizens. It is the State of fear. The State uses fear as an instrument to ascertain or validate its existence, and is at liberty to make arrangements to protect its citizens, even at the cost of their comfort. If it was cold war in the last few decades, today more current events like terrorism and Islamic fundamentalism are used to instill the fear factor. We are being changed into a surveillance society and like many other things in our life; Biometrics is advancement in science which infringes into our personal domain. Whether reservations raised by civil liberties/human rights groups are valid or not, whether the biometric technology is fool proof or not, the technology is here to stay. Today we are asked to divulge personal information such as fingerprints and retina scans for security purposes, so it would be reasonable to assume that within the next decade we could be asked for DNA. Previously, fingerprinting and DNA analysis were associated with criminals and crime scene investigations but today the same is expected of an ordinary, law abiding citizen. This brings us back to the same haunting thought – Are we guilty until proven innocent?

**References**


Biometrics an emerging technology: Market Report (2005) – U.S. Commercial Service

Biometrics gets down to business, The Economist Technology Quarterly, December 2006

Biometric Technology http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/default.stm

Biometric Technologies: Security, Legal, and Policy Implications http://www.heritage.org/Research/HomelandDefense/lm12.cfm

Biometrics 101 (Video by LTC Craig Kaucher, USA, National Defense University) http:// www.biometrics.dod.mil/bio101/10.aspx

Biometrics used to keep German Olympians safe http:// software.silicon. com/security/0,39024655,39123078,00.htm

Border surveillance plan unveiled http://news.bbc.co.uk/2/hi/technology/3700232.stm

Experts eye biometric issues http://news.zdnet.co.uk/security/0,1000000189,39181048,00.htm

Facing a biometric future http:// news.bbc.co.uk/2/hi/technology/3389209.stm

Germany to phase-in biometric passports from November 2005 http://europa. eu.int/idabc/en/document/4338/194

Let's Fight Off This National Identity Card! http://www.bbc.co.uk/dna/ actionnetwork/A13545786

Malaysia car thieves steal finger http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

My story: Thumbs down to school fingerprinting http://www.bbc.co.uk /dna/actionnetwork/A15693113

Mythbusters beats fingerprint security system http://www.youtube.com /watch?v=1sdwVlRFGdM

Safety & Security of U.S. Borders/Biometrics http://travel.state.gov/visa/immigrants/info/info_1336.html

Security Concerns and Solutions for Public Domain Biometric Applications http://www.cesg.gov.uk/site/ast/ biometrics/media/Security_Public_. pdf

US-VISIT Program http:// www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm

Walt Disney World: The Government's Tomorrowland? http:// newsinitiative .org/story/2006/09/01/walt_disney_world_the_government


**About the author**

Divya Titus received her Computer Science and Engineering degree from Chennai (India) before moving to London to pursue MSc. Analysis Design and Management of Information Systems at the LSE. Her dissertation is based in her country of residence (United Arab Emirates) where she focuses on 'The role of In-formation Systems in Islamic Banking' . After ADMIS , she will be joining JP Morgan's Business Management & Finance, and Technology Graduate Programme in UK.