David Mburu Ng'ang'a.
7th December 2005.

The Rise of Biometrics: The Effects on Society

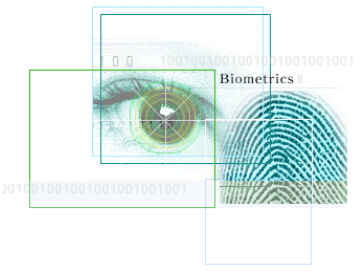
"No one seems to be concerned or particularly aware of the ramifications –threats to privacy, government and intergovernmental surveillance –that accompany biometric identification"
[By Andrea Schmidt,
Counter Punch Magazine. 10/6/2005]

"The technology has outstripped our ethical standards, our privacy standards and our legal standards"
[Scharf, Peter
Communications of the ACM, July 2002.]

"Of all the methods of identification, fingerprinting alone has proved to be both infallible and feasible"
[FBI Handbook, Wall street journal, 2005].

"Testifying about possible probable or likely identification shall be deemed … unbecoming conduct"
[The International Association for Identification,
Wall Street Journal, 2005]

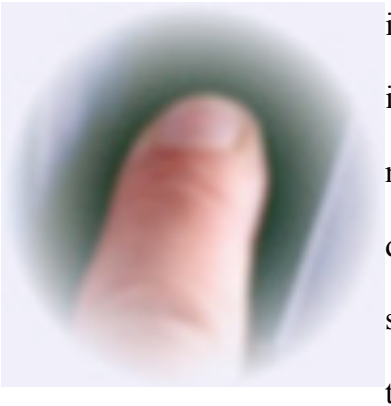
Introduction



Computer technology development in the 20th century has caused the rapid transformation of many fields. Biometrics is one such field. Biometrics can be defined as an emerging field of automated technology "devoted to the identification of

individuals using biological traits such as those based on retinal or iris scanning, fingerprints or face recognition"[Freedman,2005]. The establishment and growth of Biometrics is aimed at providing high assurance credentials for confirmation of identity. That is why Biometrics has been termed as the basis of "highly secure identification and personal verification solution" [International Biometric Group, 2005]. Each day we are faced with the challenge of identity. "Whether to solve crimes; ensure jail security; or to protect the general public, putting a name to a face can literally mean the difference between life and death" [National Identification schemes, 2005]. Biometric technology is rapidly becoming a useful tool in the security industry, especially given the view that it is tamper-resistant and serves as a solution to authenticate individuals without the need for PIN codes or additional keys to access various facilities. Biometrics systems are designed to overcome identification using passwords or PIN codes as they rely on user's physical characteristics. This is supposed to ensure that critical information does not fall into the wrong hands.

To most of us, Biometrics may seem like an infallible solution in the context of 'personal' identification, but this is not the case. Though highly accurate when identifying people in most cases, an incorrect identification is possible. Just as there is the potential for arithmetic inaccuracy in problem solving; Biometric identification is not a completely fail-safe system. Many of the Biometrics drawbacks revolve around the way the data is collected, stored, and used. At first, very few people may be willing to release their information during data collection. It is also



possible for individuals to obtain an authentic biometric credential using false identification materials such as a forged birth certificate and social security card. But what happens if a person can forge your biometric data, or tamper with your stored data, and get away with it? A significant number of people will be uncomfortable with the idea of a huge database containing their personal information at their place of work and other centralized security station. This feeds into the problem of Biometric data storage. Security experts do point out that "as more complex levels of identification and data storage are being developed, the more some people know how to break them. The security necessary to prevent people from breaking into such sensitive [personal Biometric] data is nearly impossible to achieve… Biometrics creates a personal identification risk that would otherwise not exist"[National identification schemes, 2005]. Therefore Biometric information is not as secure as one might believe, and it also suffers from a lack of standards not only in collection and storage but also in usage.

Biometric data is normally combined with other personal identification information; this raises the question as to how our information is shared. "Is it only the biometric data or is there other information in the database? And is the data available only to law enforcement agencies or can private businesses access that information? Is the data shared between governments and if so, is it shared with repressive governments" [Smith Lisa, 2005]? All these questions need to be considered as they potentially restrict personal freedoms to liberty and privacy. As long as the security necessary to prevent people from breaking into such sensitive information is not guaranteed, authenticity of personal biometric data remains at stake.

Educational Importance

The issue of biometrics usage develops into a rather complex set of questions that people have the right to know and debate before biometrics are established on National Identification Schemes [NIDs] and national security checks.

Although Biometrics provides fast and convenient levels of security check procedures such as index finger prints and iris scans at the airport, people need to be aware that biometrics are not accurate enough to trust without a backup system. The number of Biometrics applications is growing at an enormous rate and just before you realize it your company may have already installed one at the entrance! People have the right to know what is being imposed into their daily life.

Biometrics is a rapidly evolving technology which is not only being used in forensics such as criminal identification and prison security, but also in the deployment of biometric authentication in a large number of civilian applications. This has been made possible due recent advancement in Biometrics sensors and matching algorithms.

Increased security threats have made a significant number of countries to start using biometrics for border control and National ID cards. For Example the United States declared a law that says citizens of countries that lack biometric passports can no longer enjoy a waiver from the US Visa Office.

Biometrics most common use is to prevent unauthorized access to ATMs, desktops PCs, smartcards, cellular phones, and computer networks. Also it can be used to secure transactions conducted via the internet such as electronic commerce and electronic banking. As well, Biometrics is replacing the use of keys and password with key-less entry while in automobiles, key-less ignitions is very possible [Ross et al., 2005].

Personal Opinion

The expansion of Biometric technology marks a great achievement scientifically. As with most advancements, every man-made technology has advantages and disadvantages. On the one hand, Biometrics promises a more efficient world, with clear cut solutions to problems of identity, increased security and a reduced chance of fraud in business transactions. On the other hand, Biometrics brings with it a threat to personal privacy and also private personal information. Biometrics databases also hold a threat to increasing stigmatization against disadvantaged people in the society. In the prosecution of criminal cases, science has never achieved 0% infallibility; therefore there is a possibility of convicting innocent people.

Despite all the advantages and limitations of Biometrics, it is very important for people to be given a chance to express their concerns, and laws to be made that will govern the use Biometrics. Such laws will aim at minimizing harm and protecting citizens while at the same time allow utilization of Biometrics to the best.

Case Study 1

Fingerprint Matches Come Under More Fire As Potentially Fallible

FBI handbook says;

> "Of all the methods of identification, fingerprinting alone has proved to be both infallible and feasible" [Wall street journal, 2005].

Fingerprinting is the one of most widely used forms of Biometric identification. After the 2004 Madrid Bombings, some fingerprints were taken from a suspicious bag

near one of the Madrid train bombing sites. The FBI matched the fingerprints to Mr. Brandon Mayfield who is a Portland Ore lawyer and Muslim convert. Mr. Mayfield was arrested by the FBI, but after a number of investigations the Spanish Police insisted that the prints did not match Mr. Mayfield. Eventually the prints were linked to an Algerian living in Spain [Begley Sharon, 2005].

The FBI conceded the error and apologized to Mr. Mayfield. Since such an error is supposed to be impossible, the case has achieved disrepute internationally. Scientists tested the fingerprints identification, and told examiners that one set of the prints were from Mr. Mayfield and the other set from the Madrid bombings. [Begley Sharon, 2005]

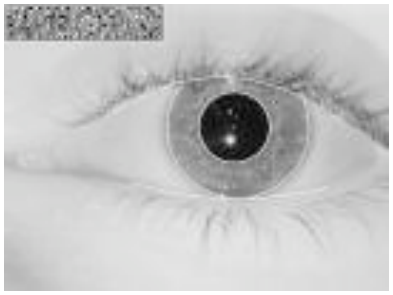
In one further investigation, one examiner said he couldn't tell if the pair matched. Three investigators said the pair did not match and pointed out why. The fifth examiner insisted that the prints – "notorious for not matching"-did not match [Begley Sharon, 2005].

Unbeknown to the examiners, the prints were not from Mr. Madrid (the Algerian living in Spain) and Mr. Mayfield. They were pairs that each of the examiners had testified earlier in a different criminal case that had come from the same person. The

three who told scientists that their pair didn't match therefore reached a conclusion opposite to the one they had given in court; another expressed uncertainty whereas in court, he had been certain [Begley Sharon, 2005]

This small study comes at a time when traditional forensic sciences - analysis of bite marks, bullets, fingerprints, hair, handwriting and fingerprints – are facing skepticism over the validity of their core claim: that when two marks are not observably different, they were produced by the same person [Begley Sharon, 2005].

Different arguments have been presented on the issue of biometrics identification For example Michael Saks of Arizona State University at Tempe says that the FBI claim lacks "theoretical and empirical foundation". He argues that forensic science has been



excused from rigorous research on how frequently attributes [ridges and whorls in fingerprints] vary and on the probability that marks with identical attributes come from different people or objects. There is no basic match on some number of characteristics that actually come from different people, as there is for DNA typing. And the data on the frequency of false matches are sparse [Begley Sharon, 2005].

In Massachusetts highest court, the unsupported and unscientific claim of infallibility is being tested. On an appeal on the infallibility of fingerprints, defense lawyers argued that the technique falls short of the standard the U.S. Supreme Court established back in the 1993 "Junk Science" decision. The decision held that scientific testimony must have a known error rate. It will be interesting to see how much longer fingerprinting can get away with "zero" [Begley Sharon, 2005].

FBI proficiency exams since 1983 find an error rate of 0.8 % .Multiplied by the millions of cases crime labs process, that works out to about 1,900 possible mismatches every year [Begley Sharon, 2005].

Case study 2

Walking the Ethical Line When it Comes to Accessing Personal Information

> "The technology has outstripped our ethical standards,
> our privacy standards and our legal standards"
> [Scharf, Peter. Communications of the ACM, July 2002.]

The ideals of a decent society say it is good to catch and put crooks, murderers, and drug dealers in jail, where they may redeem themselves. This has caused an amazingly fast and expanding array of federal, state, and local law enforcement databases throughout the US. Computer systems hold enormous amount of data which is governed and restricted by a number of laws. The existence of such data and the accuracy of the data and crime related data has a profound impact on law enforcement. The data helps determine whether police can be granted a search warrant to search a suspect's house, whether a prosecutor prosecutes or drops the case, and whether judges grant or deny bail [Scharf Peter, 2002].

The storage of this data, and the ease with which more is being collected, strikes many observers and human rights watchdogs. Such processes impose significant costs upon the poor and marginalized whenever their past records are released to prospective employers and even landlords. At this point legal and ethical frameworks must be laid out to help both law enforcement officers while minimizing harm to citizens. Currently, people's legal criminal records are becoming widely available, making it hard for these

already disadvantaged people access to apartments, employment, and education [Scharf Peter, 2002].

For Example: an article in the March 14, 2002 edition of The Wall Street Journal reported on the firing of Kimberly Kelly, a single mum employed as a pipe insulator by subcontractor Eli Lilly and Co. Kelly lost her job because she had bounced a $60 check in 2000, resulting in misdemeanor conviction. She was one of 100 contract workers banned from Lilly's sites. These 100 people are part of a much larger trend. The ease of availability of personal biometric data tagged along with other records such as medical records or criminal records pose a big threat to people's liberty and rights [Scharf Peter, 2002].

Key Words.

- Biometrics- Implementing identity related technology [Dictionary.com, 2005].
- Forensics - relating to the application of science to decide questions arising from crime or litigation; forensic evidence [Dictionary.com, 2005]
- Authentication- Confirmation, certification; To establish the authenticity of; prove genuine [Dictionary.com, 2005]
- Identification-The act of identifying; the state of being identified; *Abbr.* **ID** Proof or evidence of identity [Dictionary.com, 2005]
- Verification- Involves the confirming or denying a person's claimed identity. The act of verifying or the state of being verified [Dictionary.com, 2005]
    - A confirmation of truth or authority.
    - The evidence for such a confirmation.
    - A formal assertion of validity.
- Credentials- That which entitles one to confidence, credit, or authority; Evidence or testimonials concerning one's right to credit, confidence, or authority [Dictionary.com, 2005]
- Scanning- To examine closely. To look over quickly and systematically. To move a finely focused beam of light or electrons in a systematic pattern over (a surface) in order to reproduce or sense and subsequently transmit an image [Dictionary.com, 2005]

Works Cited

- Begley, Sharon (2005). Fingerprint Matches Come Under More Fire as Potentially Fallible. Science Journal. Wall Street Journal. Friday October 7, 2005 Newsletter. Dow Jones and company, 2005

- "Biometrics." National identification schemes. 11 Sept. 2005 <http://www.cspr.org/issues/privacy/natafiq.>.

- "Biometrics." The international biometric society. 16 Sept. 2005 <http://www.aliconferences.com/conferences/biometricssummit105/1105.html>.

- Freedman, Lin, and Kenward (2005). "Biometrics." The international Biometric group. 15 Sept. 2005 <http://tibs.org/biometrics/>.

- Lexico Publishing Group, LLC. Dictionary.com.
  Dictionary - Thesaurus - Encyclopedia – Web. 6th December 2005.
  <http://dictionary.reference.com/search?>

- Munro, Neil (2002). The Ever expanding Network of Local and federal databases. Communications of the ACM journal, July 2002. ACM publications Office, 2002.

- Ross, Arun, Salil Prabhakar, and Anil Jain (2005) "An overview of Biometrics." Biometrics. 06 Sept. 2005 <http://biometrics.cse.msu.edu/info.html>.

- Scharf, Peter(2002) Walking the Ethical Line When it comes to Accessing Personal Information. *Communications of the ACM*, July 2002.
  CAM publications office, 2002.

- Schmidt, Andrea (2005). "A high tech experiment in Exclusion.
  Haiti's Biometric Elections, 2005"
  <http://www.counterpunch.org/schmidt10062005.html>

- Smith, Lisa (2005). "Biometrics: privacy and civil liberties." 11th September 2005.
  <http://www.cpsr.org/issues/privacy/natIdentity/Biometrics>