AC 2012-3789: ETHICAL AND SOCIAL CONSEQUENCES OF BIOMETRIC TECHNOLOGIES

Dr. Rigoberto Chinchilla, Eastern Illinois University

Rigoberto Chinchilla, PhD in Integrated Engineering, Ohio University, is an Associate Professor of Applied Engineering and Technology at Eastern Illinois University (EIU) since 2004. His teaching and research interests include Quality design, Biometric and Computer Security and Ethics, Clean Technologies and Automation. Dr. Chinchilla has been a Fulbright Scholar and a United Nations scholar, serves in numerous departmental and university committees at EIU and has been awarded several research grants in his career. Dr. Chinchilla Publications in 2011 include

oChinchilla, Rigoberto, Harris, Harold, Facial Recognition System Screening Evaluation Methodology for Complexion Biases: Proceedings of the 2011 American Society for Engineering Education ASEE, Conference. Vancouver Canada, June 26-Jun30 2011

oChinchilla, Rigoberto, S. Guccione, J. Tillman, Wind Power Technologies in the United States: A Technical Comparison between Vertical and Horizontal Axis Wind Turbines: Journal Of Industrial Technology Volume 27, Number 1 - January 2011 through March 2011

Dr. Chinchilla can be reached at rchinchilla@eiu.edu.

Ethical and Social Consequences of Biometric Technologies in the US

Abstract

Biometrics can be defined as all the authentication techniques relying on measurable physiological and individual human characteristics that can be verified using computers. This paper outlines fundamental biometric technical concepts, biometrics drivers, security expectations and current technical problems. The paper's main objective is to discuss the potential social and legal consequences of biometric massive implementations in society. What may be the consequences when the security of our biometrics is compromised? How will populations with disabilities be enrolled in biometric databases when they lack the physical traits the biometric system requires? Are minorities disadvantaged in biometric applications? The intellectual significances of this paper are: (a) to discuss social and ethical consequences of biometric technologies, and (b) to increase public awareness of potential violations of privacy, security, civil and human rights that may have not been fully addressed yet by lawmakers. The findings of this paper have been successfully incorporated in courses related with engineering ethics and technology ethics at a senior level and graduate level. Results of these implementations are presented.

Biometrics Fundamentals

Human beings have unique physical and behavioral attributes that can be used for authentication purposes. Authentication is a process that leads us to have a high degree of certainty or probability about the identity of an individual. Biometrics can be defined as all the authentication techniques that rely on measurable physiological or behavioral human characteristics that can be verified using computers. Authentication can be done by comparing the biometric information an individual gives to the computer against a binary record previously stored in the computer called template.

If the computer makes a comparison against one and only one template in order to match the physical or behavioral characteristics of an individual, the authentication process is called verification. In the verification process, the individual is the one who claims a specific identity. Verification applications are typically aimed to allow individuals the right to access a facility or to use a resource. If the computer makes a comparison against all its templates in order to find if the individual belongs to the template's database, the authentication process is called identification. In the identification process, there is no previous claim about an individual's identity. Identification applications are typically used by forensics, crime investigation and security applications.

A biometric can be broadly classified as behavioral (i.e. Signature, Gait, Lip motion) or physiological (i.e. Fingerprints, Iris, Face, Hand geometry, Retina). In order to build a biometric application, the first step is to enroll the potential users of the application in a database. Enrollment is performed by using electronic sensors and complex mathematical algorithms capable of detecting and capturing the physiological or behavioral characteristics of the individual. After the image representing the biometric characteristic of an individual is captured, a set of vendor proprietary algorithms are in charge of processing the image in order to convert it to a template. Therefore different vendors will have different binary representations and accuracies of the biometric upon the quality of algorithm(s) and the sensor(s) used.

Biometric systems compare templates based on probabilistic processes. When an individual wants to access a facility, a biometric sample is provided resulting in the creation of a sample template. This template is then compared with the stored template in the algorithm's database. In biometrics, a score is a number that results from the statistical comparison of two templates. The score represents the probability that two templates belong to the same individual. The biometric systems administrator has to setup a score threshold to which the samples will be compared. Typically, if the statistical score from the sample template is greater than the score threshold, the biometric system concludes that the sample-template and the one stored in the database belong to the same individual. If the sample score is below the score threshold, the biometric system concludes that the two templates are statistically different and the individual does not belong to the database.

Biometric systems are not 100% accurate. Biometric systems accuracy during the template comparison process of authentication depends on external variables, namely, temperature, training level of the enrollment process technicians, physical condition of the individual to be authenticated, etc. Biometric systems accuracy is also dependent on internal variables such as quality of the equipment and the proprietary algorithms being used. Most biometric systems derive their fundamental accuracy from the following parameters[1]:

- False Match Rate (FMR): Is the probability that an imposter will be accepted as a genuine user by incorrectly judging a match in his or her enrollment template
- False Non-Match Rate (FNMR): Is the probability that a genuine user will be rejected by incorrectly judging a mismatch in his or her enrollment template
- Failure To Enroll (FTE): Is the probability that a given user will be unable to enroll in a biometric system

FMR and FNMR are dependent variables and their relationship to one another can be described by the Receiving Operating Characteristic Curve (ROC) shown in Figure 1[2].

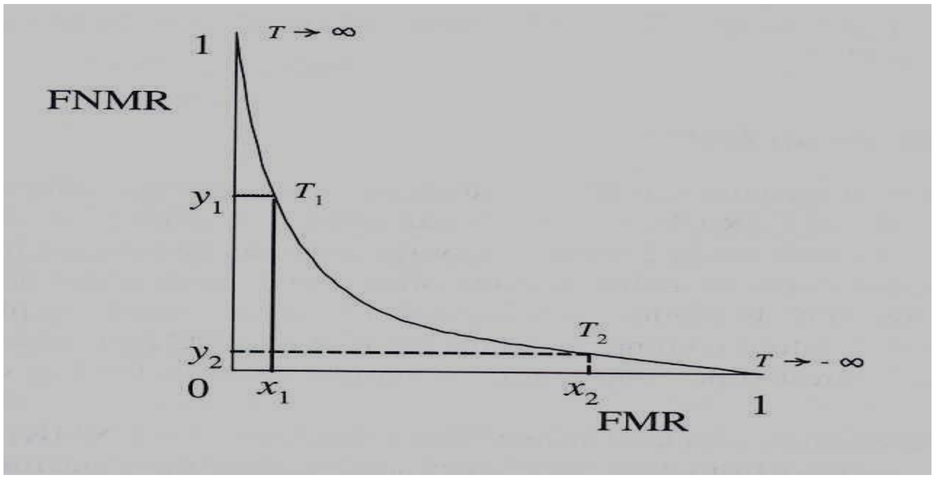

Figure 1: ROC curve[2]

By looking at Figure 1, it can be concluded that the lower the probability that imposters can be accepted as a genuine users (i.e. “x_1”, low FMR implies high security), the higher the probability that genuine users will be rejected (i.e. “y_1”, high FNMR implies inconvenience for genuine users). Conversely the higher the probability that imposters can be accepted as genuine users (i.e. “x_2”, high FMR implies low security) the lower the probability that genuine users will be rejected (i.e. “y_2”, low FNMR implies convenience for genuine users). In biometric systems, a trade-off between security and convenience is always present; any setup of the operating point (i.e. “T_1” or “T_2”) will inherently modify the relationship between the FMR and the FMNR. Accuracy and performance may diminish as the one-to-many relationship database size increases, this situation may require human intervention via exception handling to make a positive identification.

Biometrics Drivers and Expectations

Biometric technologies have been with us for several decades; yet the massive implementation of biometric security applications has recently surged as one of the responses to the September 11 attacks on the United States (US). It is believed by government agencies, the media and public in general, that a massive implementation of biometric applications will increase the security of the US population. Powerful computers, cheap memory, sophisticated databases, digital images, and available communication bandwidth are the main biometric application drivers.

Besides increased security, biometrics gives convenience; data can not be guessed or stolen in the same fashion as a password or token. Although it is known that some biometric systems can be broken under certain conditions, most of today’s biometric systems are highly unlikely to be fooled by a simple impression of a fingerprint, a picture of a face, or a recorded voice[3]. Typically, the level of security provided by most biometric systems far exceeds the level of security provided by passwords, PINs or tokens. Most biometric systems have strong auditing and reporting capabilities. By correctly identifying individuals who have already registered for a program or service, biometrics technologies can reduce fraud. Fraud deterrence is probably one of the major benefits of biometrics, the very presence of biometrics dissuades many people who might otherwise be prone to attempt multiple registrations, and this helps to ensure the integrity of the records[3].

Technical Problems with Biometrics

Typically, the weakest link in a biometric system is the enrollment process. A subject can create a new identity by presenting fake documents (i.e. driver’s license and or passport) during the enrollment process in a biometric facility. Once a new fake identity has been accepted, an imposter can board a plane, enter a facility or buy restricted materials. When biometric databases are not interconnected, it is entirely possible to steal a genuine identity by presenting another person’s documents during the enrollment process. It is a known fact that some of the September 11 attackers possessed up to a dozen US valid driver licenses with different identities[4]. If a government can not guarantee the emission of documents to imposters then a biometric system will do little or nothing to increase security and/or maintain the integrity of the databases.

There is not yet a world-wide acceptance of what quality means in a biometric sample. The International Committee for Information Technology Standards (INCITS) in the USA defines quality by three parameters: character, fidelity and utility[4]. The character of a biometric is mostly related with the intrinsic physical condition of an individual (i.e. an individual whose fingerprints have been deteriorated by abrasives, has fingerprints with "poor biometric character") [5]. Fidelity is defined as the accuracy by which physical characteristics are represented in a sample; fidelity is highly dependent on sensors and algorithms that capture the sample. Finally, utility is defined as "how valuable is the sample for a given purpose" [5]. INCITS has developed a scale for each of the three parameters. A current problem is that many biometric vendors neither rely on the INCITS quality definitions nor on its scales.

Another major problem within the biometric industry is the lack of mature standards. Mature standards ensure that vendors comply with common authentication protocols, use common biometric exchange file formats, share common scales of sample quality and develop a common protocol for equipment conformance testing. International committees on standards like the International Standards Organization (ISO) and the US counterpart (INCITS) have developed the BIOAPI standard aimed to fulfill the lack of industry standardization[6]. By December 2011, only about 50 vendors claim to comply with the BIOAPI standards but the BIOAPI consortium can't verify if they really comply[7]. Legacy biometric equipment that does not conform to the BIOAPI standard is installed in many facilities in the US. The lack of well-trained personnel to manage biometric facilities, the different accuracy of the vendor's mathematical algorithms and users not well-informed about biometrics, are a set of problems whose consequences are not yet fully addressed. There is a movement aimed to build databases using legacy databases (i.e. use of the driver's license photos in legacy databases to build a face recognition application). If a legacy database contains many imposters, their direct use for biometric applications will result in a decrease in security for the US population.

Building massive biometric applications in society requires a critical mass of technicians capable of managing the applications properly. Typical activities of these technicians are to collect samples for enrollment using complex sensors, to authenticate identity documents (i.e. passports or birth certificates) of individuals before enrolling them, maintain the biometric facility under proper conditions, follow maintenance protocols properly and judge the quality of the samples collected. Technicians who are not well trained can hinder the expected security level of a facility. There are very few technical and professional schools at this moment capable of training the required quantity of technicians with the expected quality. Most biometric technicians are trained onsite by the vendor's personnel.

Social Consequences of Biometric Applications

Biometric technology, like any other technology, suffers from unexpected and unforeseen consequences that many other technologies have experienced when implemented in society. Problems can arise when massive implementations are done. What happens when a biometric file is stolen? A password or a credit card can be relatively easy replaced and the stolen information somehow invalidated. A biometric template is nothing more than another binary file in a database, therefore can be stolen by hackers as any other file. Losing our own biometrics may not be a matter of replacement; "with a biometric it is very difficult, if not impossible, for any individual to disassociate oneself from one's biometric"[8]. If biometric databases are not protected properly and information is stolen, the consequences can be permanently devastating. There is no easy way to program the biometric systems to not recognize a legit biometric of an authentic user. Once the standards are in place and biometric systems are interconnected around the world, a stolen biometric can be used improperly (i.e. by using telecommunication channels) with massive damages to the public.

What happens when biometric is used for surveillance purposes? Face recognition surveillance may be used for security purposes to monitor well-known criminals. Faces can also be captured from social websites, sporting events, concurred streets or malls and used for non-related security purposes without people's consent in clear violation to the individual's right to privacy: "If there is any 'law' in the history of technology it is that technologies are rarely used in ways that their inventors intended" [7]

Are minorities disadvantaged in biometric applications? It has been seriously suggested that many biometric applications are biased toward certain minorities. The Face Vendor Recognition Test (FRVT), organized by the US government in 2002, showed that identification rates for males were 6% to 9% points higher than that of females and recognition rates for older people were higher than younger people[7]. Based on the FRVT of 2002 Givens,[9] also concluded: "Asians are easier (to recognize) than whites, African-Americans are easier than whites, other race members are easier than whites, old people are easier than young people, other skin people are easier to recognize than clear skin people…". Therefore the multiplicity of algorithms in the market may be designed with inherent and unforeseen biases. If biases are proven, it will make the use of these systems illegal and unethical, especially when social services or access to public facilities (like the right to enter a public park or stadium) are denied to minority groups when falsely rejected them in higher proportions with respect to other groups based on their race, color or gender.

How will population with disabilities (or lacking physical traits) will be enrolled or authenticated in biometric databases? People with just one hand, no iris or retina, no fingers, and in general people lacking physicals characteristics in need of using a biometric facility, may suffer discrimination and unnecessary delays in biometric systems. A well-developed, well-designed biometric system should allow these persons alternative ways to enroll and authenticate, yet delays and processes of bypassing the biometric systems may give them hardships each time they want to access a resource or use a facility which may be an ethical violation of their rights.

Finally, lack of mature standards and standardization enforcement may create a different set of results for similar facilities located in different geographic sites requiring similar sets of security requirements. Lack of proper standardization has the potential to discriminate users based on the geographic biometric facility they want to use. A user may be well-recognized in one facility but rejected in another one without major explanation.

The US government is promoting contests among vendors in order to motivate them to comply with standards and to improve their equipment accuracies but so far this is a voluntary activity. Eventually most vendors in the US will comply with standards. The US government is mostly conducting business with vendors who comply with the BIOAPI standard, yet privates companies are free to install any other system without standard enforcements. Confusion from the public and discrimination in general will be some of the major social consequences when there are no mature standards and/or the adoption of a common standard by most vendors is not enforced.

Legal Consequences of Biometric Applications

Democratic societies value individual privacy as well as government accountability. The rule of law shapes the manner by which the government may interact fairly with its citizenry[10]. The two fundamental legal principles related with Biometric technologies are the due process and the right of privacy:

> "The concept of due process requires the government to acknowledge the possibility of errors, allowing means for their mitigation. The concept of privacy goes beyond simply acknowledging the possibility of errors to set limits on the power of government to meddle in the lives of individuals. These court protected guarantees require the government to respect the right of individuals by limiting intrusions to those which directly further recognizable and legitimate societal interest. This historical balance between individual rights and societal interest is at the heart of all democracies, and is placed under a new strain by the advent of biometric technologies"[11].

The fourth, fifth and fourteen US constitutional amendments[12] are the ones related with privacy, due process and security. The fourth amendment protects against unreasonable searches and seizures, the fifth and the fourteen amendments ensure the due process to protect citizens. The logic of due process is rooted in the notion that personal freedom in a constitutional democracy can only be preserved when there is some consistent way to check arbitrary and capricious actions by the government[13].

There are two approaches in order to guarantee due process. The first approach, the intrinsic approach, consults the citizens before implementing an action that may violate their rights. In the intrinsic approach, citizens are more informed and can modify proposals and study the consequences of the law before the law applies to them. The second approach to due process, the instrumental approach, does not focus on the right of the citizens to be part of the decision-process making when implementing a law. The focus of the instrumental approach is to ensure that the right procedures created by the government have been followed; the public have the right to due process if and only if the processes in place have not been followed. According to Nuger and Wayman, the instrumental approach is the one that have been used in the last 25 years in the US society in disfavor of the intrinsic approach[11].

The implementation of biometric technologies has followed the instrumental approach in the name of security; citizens have been passive subjects, willing to accept whatever biometric technology is imposed to them in the name of security. The public, at the same time, has not been properly informed of all the social and legal consequences of these implementations. Once lawyers and the general public begin to understand the weaknesses of these technologies a wave of legal litigation may be expected when biometric systems are implemented in all areas of society. The right to privacy protected by the fourth amendment may be in jeopardy by the massive application of biometric technologies. Surveillance is a perfect example in which the balance between public security and the right to individual privacy may be at the hands of people who favor the sharing of biometric information with different purposes other than ensuring public safety in clear violation of the fourth amendment.

The "reasonable search" part of the fourth amendment has been the subject of profound, not yet solved, legal battles before biometric technologies appeared in society[14]. With the implementation of automatic and instant methods to recognize people and the pace at which biometrics technology is changing, citizens often do not have time to react and ensure their rights have not been violated. The "Facebook" and "My Space" generations seems to do not mind sharing not only personal information but also biometric information publicly, making it extremely easy for anyone "in the network" to gather biometric information. Social consequences brought by biased algorithms discrimination, hacked databases and not well-understood privacy policies in surveillance or in social websites containing biometric information undoubtedly will carry profound legal consequences.

Academic Programs: Biometric and Ethics

ASEE has a strong recommendation about integrating ethics in engineering education[15] either in each course or in a separate engineering course, but there is no specific number of hours recommended. The author recommends that engineering graduate and undergraduate courses in biometric security, automatic recognition and emerging technologies devote substantial time to discuss the social/legal consequences of biometric technologies. In my biometric courses, I invest about 5 hours (~10%) of the total course to discuss Ethics and legal consequences of biometric technologies. If the course is not directly related with biometric engineering and/or technology or additional knowledge needs to be induced in our students these can be done by means of homework and/or final papers.

The author has implemented a five-hour ethics seminar in graduate courses like "Emerging Technologies" "Biometric security", 'Global Technology" and an undergraduate course "Technology and Society". The seminar syllabus contains: A discussion of what biometric is and the core of the technology (i.e. recognition algorithms), practical implementation problems, problems with standards and enrollment, social and legal consequences of the technology with emphasis in the fourth, fifth and fourteen amendments of the US constitution. After the seminar, students take a quiz on basic ethics and the issues related with biometric technologies then within a week they have to write a brief "field report" on specific examples about the use of biometrics around or in campus. About 90% of the students have successfully passed the exam on basic ethics, 100% of them have written a report on standards and about 30% of them have decided to write a final paper related with Biometrics and ethics.

If a separate course in engineering ethics is taught, I will strongly recommend the inclusion of "Biometric Ethics" in schools of Electrical Engineering and/or Computer Science. It has been argued that the best way to teach ethics in engineering is by using "cases of study" [16]; In the case of Biometrics those cases of study are yet scarce, however we can cite at least three documented cases worthy of analysis (all of them related with privacy issues) as cited in references

Conclusions

Unforeseen and unexpected consequences are the constants when implemented a new technology, biometric technology, like any other technology is not the exception. Many other technologies have experienced similar patterns of problems when implemented massively in society. Any technological advance or technological change requires a period of social acceptance that, for biometric technologies, has been shortened in the name of security; no technology can be implemented massively without a social cost. The use of any technology without understanding the consequences to the public are intuitively unethical. Most technologies follow the same pattern of unknown consequences pushed either by massive consumerism, or in the case of biometrics, by using security as the main driver. The social and ethical consequences that biometric technologies may bring to the public are not yet fully discussed and society has not been informed of their potential damages.

References

[1] NIST, "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability." Nov 2002; http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf
[2] R.Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, "Guide to biometrics". Springer-Verlag, ISBN o-387-400-89-3, 2004
[3] S. Nanavati, M. Thieme, R.Nanavati, "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, ISBN 0-471-09945-7, 2002.
[4] Expert: Hijackers likely skilled with fake IDs **http://articles.cnn.com/2001-09-21/us/inv.id.theft_1_hijackers-identity-theft-social-security-numbers?_s=PM:US** [Accessed Dec 26, 2011]
[5] NIST, "NIST/ITL's Biometric Application Programming Interface (BioAPI) Conformance Test Suite (CTS)**",** September 3, 2008**;**
[6] BioAPI consortium, "Version 2.0 of the BioAPI Specification - International Version", 2006; http://www.bioapi.org/Version_2.0_Description.asp
[7] BioAPI Consortium, "Related Products" http://www.bioapi.org/products.asp [Accessed Dec 26, 2011]
[8] L. D. Introna, D. Wood, "Picturing Algorithmic Surveillance: The Politics of
Facial Recognition Systems", *Surveillance & Society*, ISSN Number: 1477-7487, 2004; http://www.surveillance-and-society.org/articles2(2)/algorithmic.pdf
[9] Givens, G., J.R. Beveridge, B.A. Draper and D. Bolme, (2003), *A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces.* http://www.cs.colostate.edu/evalfacerec/papers/csusacv03.pdf [Accessed Dec 22, 2010]
[10] W.H. Simon, The legacy of *Goldberg v. Kelly:* a twenty year perspective: the rule of law and the two realms of welfare administration. 56 *Brooklyn Law School 777* (1990)
[11] J. Wayman, A. Jain, D. Maltoni, D. Maio, "Biometric Systems: Technology Design and Performance Evaluation". Springer-Verlag London Limited, 2005.
[12] Find Law, For Legal professionals, US constitution amendments http://caselaw.lp.findlaw.com/data/constitution/amendments.html [Accessed Dec 26, 2011]
[13] S.H. Kadish, methodology and criteria in due process applications- a survey and criticism. 66 *Yale Law journal* 319 (1957)

[14] The 'Lectric Law Library's Legal Lexicon On * FOURTH AMENDMENT*. http://www.lectlaw.com/def/f081.htm [Accessed Dec 26, 2011]

[15] “ASEE Statement on Engineering Ethics Education” http://www.asee.org/about-us/the-organization/our-board-of-directors/asee-board-of-directors-statements/engineering-ethics-education [accessed Dec 26, 2011]

[16] Harris, Davis, Pritchard and Rabins, “Engineering Ethics: What? Why? How? And When?” Journal of Engineering Education” (pp. 93-96, April 1996)