Paper 10 Proceedings of 8th International Engineering Symposium at Bánki [PDF] (ISBN: 978-615-5460-95-1), 2016

# Biometric Information Acquisition, Privacy Issues at the Workplace: Monitoring versus Security

**Lourdes. C. Ruiz. S[1], Tibor. Kovács[1]**

[1]Obuda University, 1034 Budapest, Bécsi út 96/B, Budapest Hungary

**Abstract.** Biometric Systems have become relevant in the workplace as a valuable tool to ensure safety and employee monitoring. However, privacy issues concerning biometric data acquisition are raising the attention of employees. The following paper will analyze the main privacy concerns, data protection laws, factors to be considering along the implementation of a biometric system and possible solutions in order to develop a healthy balance between monitoring and safety.

**Keywords:** Biometrics; Privacy; Workplace; Safety

## 1 Introduction

Biometric technology is a powerful tool for businesses. It uses biological characteristics to effectively identify an employee. Biometric systems can be divided into two groups:

- Identification systems consist in the confirmation of a person's identity by comparing biometric information templates stored in a database with the template of an unknown person [1].
- Authentication/ verification systems comprise two steps: 1. Enrollment, the biological trait is acquired; the distinctive features are extracted and stored in the database as a template. 2. Identification, the individual presents the biometric characteristic, which is compared against the features previously stored as a template [2]

Figures 1 and 2 explain how the two types of biometric systems work.

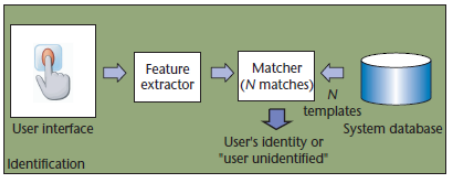


Figure1: Diagram of a Biometric Identification System. Source: [3]

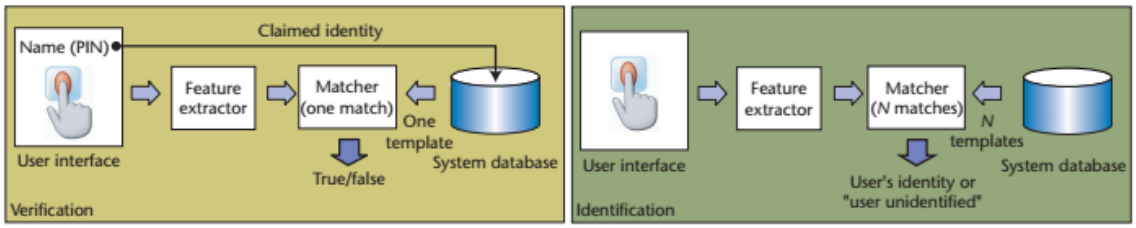


Figure2: Diagram of Authentication/Verification System: Enrollment and Verification Step. Source: [3]

Biometric data serves for various purposes such as: monitoring employees' movements, keep track of processes, record work hours, protect sensitive material, information, prevent fraud, misbehavior, grant access to employees to specific areas, computer networks and restrict access to unauthorized personnel into company's premises [4].

Biometric characteristics are unique for each person, and cannot be changed through time. Concerns about the use of the data, the possibility of information theft or biometric equipment spoofing; raise concerns among employees. Companies are relying on their security by implementing biometric systems which creates a conflict between workers. The following document will address privacy issues, laws regarding personal data and provide guidance about the execution of biometric systems in the work place.

## 2 Biometric Identifiers and Privacy Issues

Biometric data can be a physical characteristic such as: fingerprint, palm, iris, retina, face, ear structure, DNA, hand vein, odor or behavioral such as: keystroke, signature, and gait [5]. Moreover, during employee wellness or health management programs, biometric screenings are conducted by the acquisition of blood pressure, height, weight, body fat, cholesterol and glucose levels [6]

These biological attributes are intrinsic for each individual, they can establish a person's identity and reveal sensitive information that the employee doesn't want to share. Characteristics can be acquired in different situations such as: threatening the individual, when she is unconscious and without the person's knowledge; implying a threat to her safety and privacy [7]. The usage of biometric identification in different aspects of an individual's life can leave a trace of personal information. Privacy concerns such as misuse of the information, biometric data safety and the possibility of sharing, stealing and connecting biometric identifiers with private data among different databases prevent employees to accept biometric systems. Workers believe that biometric technology is invasive and they are losing control over their personal data [3].

Specific biometric traits can show data related with previous medical treatment, present, future medical conditions and non-disclosed disabilities [8]. Diseases such as gout or arthritis can be identified by hand geometry recognition; fingerprint patterns can show chromosomal disorders [9]. Eyes can reveal health problems such as heart failure,

cholesterol levels and anemia. Pupil responses can detect drug consumption or pregnancy [10]. Eye retina blood vessels patterns determine aging and can change due to certain illnesses such as type 2 diabetes, hypertension, stroke or a cardiovascular condition [11]. Previous medical treatment such as cataract surgery can affect iris pattern recognition and false rejection errors can increase [12]. In addition, voice or facial identification can show anger, stress or nervousness. Employers can use this data to identify workers' emotional health. Moreover, errors in biometric enrollment and recognition can occur due to previous medical conditions. They can also prevent workers to be included in a biometric system [13].

Biometric data can determine if a worker had a medical condition by comparing data extracted at the enrollment process with data acquired at the recognition steps. Surgeries, dental reconstruction, implants, scars and tattoo removals can be spotted by infrared cameras used for biometric collection [8]

Furthermore, sensitive medical data can result in discrimination during hiring processes and access to health insurance. An employer can consider an applicant with previous illnesses or medical predisposition as a cost for the company in medical bills, absences and productivity [8]

## 3 Data Protection Laws

Employees' concerns regarding privacy or identity theft are considered very serious. Biometric information is protected through different laws depending on the country or the region.

In Canada, the federal law that refers to the usage, collection and disclosure of personal identifying information uses the "reasonableness" principle which recognizes the usage of biometric information as reasonable when the employer has advanced a legitimate business interest and the interference on the employee's privacy is minor [14].

In United States biometric laws differ from state to state. For example, in Texas and Illinois it is required to give a notice and an individual consent before biometric collection, stating the purpose, length, use and storage of the acquired data. It is not allowed the use of biometric characteristics for commercial purposes. Furthermore, companies should have a written policy in relation to the retention and destruction of collected biometric data. The retention is limited and the destruction is obligatory after its intended purpose. Biometric information disclosure without consent is possible if requested for a financial transaction, applicable law or a warrant. Businesses should protect the collected information using industry standard reasonable care and treat biometric data as confidential and sensitive information. Moreover, for enforcement actions these laws include fines of $1000, $5000 and up to $25000 per violation and damages.

States such as: California, Washington, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, Wyoming and New York, presented laws considering biometrics as personal information which includes the application of security measures to protect the data and notification as a requirement [15].

European Union (EU) data protection laws, dictate standards for transferring and protecting the data collected by biometric or monitoring technologies. Data protection principles such as anonymity, proportionality and purpose should be used for biometric managing systems. The Data protection act states that data "shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed", "data shall have been obtained and shall be processed, fairly" [16]. Forthcoming biometric laws within EU will evolve from personal data protection into societal data protection by enhancing data and identity management [17].

## 4 Biometric Systems Implementation in the Workplace

Despite privacy issues described above, companies are relying more in biometric systems for providing security in the workplace. Benefits of the introduction of this technology surpass its flaws. Employees' legitimate concerns related to the use of their personal information should be addressed along with the designing and implementation of a biometric based system.

Consequently, there are some guidelines and regulations that should be taken into account in order to solve the conflict generated between biometric acquisition and private data protection. These are:

- *Purpose and Proportionality*: These principles should be followed before introducing a biometric system. An analysis of whether the collection of biometric data is necessary or other less intrusive measures can be taken to serve the same purpose should be analyzed [8].
- *Environment:* It is important to identify if the workplace needs high security levels, due to sensitive information or dangerous materials storage. These factors require the implementation of biometric recognition systems.
- *Notification:* Before any data acquisition process, it is necessary to send a written notification to the employees stating the purpose, potential purposes, usage, retention, disclosure and data safety procedures that will be taken in place during the biometric [16].
- *Multimodal Methods:* Consider the usage of biometric characteristics in conjunction with other gadgets such as smart cards, keys or digital signatures to increase safety [18]
- *Education:* Inform and explain to the employees how the technology works. Therefore, they will know that their personal data is protected and be willing to be part of the acquisition process. Biometric scanning devices do not store the biological characteristic just a digitized template that is encrypted which

guarantees that the characteristic will be only used for that specific application [3].

- *Data protection laws:* Identify and be aware of privacy and data protection laws that are relevant for the region or the area where the system is going to be implemented.
- *Consent:* Employees' consent is advised in order to comply with fair obtaining and processing provisions.
- *Information Security:* Design, implement and enforce security policies and processes that ensure that the collected data is safely stored and protected [19]. It is advised to use a decentralized biometric system for storing the information [20]. Minimum information safety standards comprise:

  -Access to the information is limited to authorized personnel

  -Computer systems need to be password protected

  -Back-up and disposal procedures should be established and implemented

  -Workers should be aware of the security practices and comply with them.

  -A person should be in responsible for checking security procedures compliance and enforcement [16].
- *Retention:* procedures ensuring that biometric traits will not be retained longer than from the intended purpose should be enforced. Policies regarding the elimination of biometric traits of an employee that has been permanently removed from her job duties should be taken in place [16].
- Plan a system that will be able to accommodate employees' requests regarding issues such as religious beliefs or disabilities [19].
- *Accuracy*: procedures regarding accurate identification through time should be included during the implementation of the system [16].

# 5 Conclusions

Biometric Systems are becoming more popular in the workplace because they present security advantages compared with conventional methods such as passwords, pins, tokens or keys and also can be used together without the need of replacing the previous technology. The usage of a biological characteristic can be considered an improvement of these traditional methods.

Biometrics is the science of identification based on who you are instead of what you know. The usage of human's intrinsic characteristics for identification purposes enhances security but also raise awareness of the usage of personal information and privacy. For these reasons, it is vital to follow certain guidelines described above during the whole biometric acquisition process.

It is important to comply and enforce laws related to data protection but it is necessary to focus on the ethical implications that come when acquiring biometric characteristics. Acknowledging the employee's fundamental right to privacy.

Data protection should be priority number during the implementation of biometric systems. It should be considered the heart of the system since most privacy issues are related to the possibility of misuse, lost or stolen information. If a good data protection system is taken in place, biometric characteristics can be a vital tool to protect workers and the company instead of being the source of privacy infringement.

Data protection laws are an excellent way to enforce safety procedures towards personal data protection. Strict penalties and fines for privacy violations in the workplace will take off in some extent workers' concerns about biometric collection and usage.

It is important to consider the usage of a non-invasive method that can serve the safety purposes and contributes to efficient processes, before implementing a biometric acquisition system that jeopardize employees' privacy and can be the source of discrimination. Finding the balance between workers' monitoring and security should be the key of a successful security system.

Employee tracking technologies such as Global Positioning Systems (GPS) or Radio Frequency Identification Devices (RFIDs) raise privacy concerns since the employer can know the worker's exact location at any time including non-working hours. This topic is outside the present document scope but it needs to be addressed in order to offer better tracking solutions.

There is not a perfect biometric characteristic that can be reliable and solve privacy issues. Biometric systems implementers have the challenge to choose the biometric identifier that suits better to the specific application in the system

Consent biometrics is becoming a hot topic among biometric system users due to safety reasons. Users can access to biometric guarded facilities with threats or in unconscious states. For these reasons, liveness test should be also part of a workplace biometric system. In order to solve this problem, source [7] proposes a consent signature based on behavioral information.

## 6 References

[1] "Data Protection Comisioner Ireland," [Online]. Available: https://www.dataprotection.ie/docs/Biometrics-in-the-workplace/m/244.htm. [Accessed 6 October 2016].

[2] Directorate for Personal Data Protection Macedonia, "Guidelines regarding the

Introduction of Biometric Data".

[3] J. Anil K, R. Arun and P. Salil, "An Introduction to Biometric Recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*, 2004.

[4] M. James, "10 Ways Biometrics Technology Can Make your Workplace Safer," 11 September 2009. [Online]. Available: http://ezinearticles.com/?10-Ways-Biometrics-Technology-Can-Make-Your-Workplace-Safer&id=2908729. [Accessed 22 April 2016].

[5] A. K. Jain, A. A. Ross and K. Nandakumar, Introduction to Biometrics, ISBN : 978-0-387-777326-1, New York: Springer, 2011.

[6] American College of Occupational and Environental Medicine, "Biometric Health Screening for Employers," *Journal of Occupational and Environmental Medicine,* vol. 55, 2013.

[7] Y. Kai, Y. D. Eliza and Z. Zhi, "Consent biometrics," *Neurocomputing 100,* pp. 153-162, 2013.

[8] R. J. Minter, "The Informatization of the Body: What biometric technology could reveal to employers about current and potential medical conditions," in *American Bar Association, Labor& Employment Law Section National Conference on Equal Employment Opportunity Law*, New Orleans, 2011.

[9] J. D. Woodwar, W. Katharine, E. Newton and M. A. Bradley, Army Biometric Applications, RAND Corporation, 2001.

[10] Select Commitee on Science and Technology United Kingdom, "Structure of Identity Cards Programme," Parliament UK, 2005.

[11] T. Nguyen, "Retinal Vascular Manifestations of Metabolic Disorders," *Trends Endocrinol Metab,* vol. 17, 2006.

[12] R. Roizenblatt, P. Schor, F. Dante, J. Roizenblatt and R. Belfort Jr, "Iris recognition as a biometric method after cataract surgery," BioMedical Engineering Online, 2004.

[13] Danish Biometrics, "Biometric Identification Technology Ethics," 2003.

[14] J. Crews and A. Ebejer, "Security at Your Fingertips: Biometrics and Workplace Law," Actual iD, 2015.

[15] S. Castic, S. G. Leitch, A. Swaminathan and A. P. Kim, "Orrick," 4 March 2016.

[Online]. Available: http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/. [Accessed 2 October 2016].

[16] Data Protection Commissioner Ireland, "Biometrics in the workplace," Data Protecion Commissioner.

[17] A. Sprokkereef, "Data Protection and the Use of Biometric Data in the EU," in *The Future of Identity in the Information Society*, Springer, 2008, pp. 277-284.

[18] Growth Business UK, "Growth Business UK," 20 June 2005. [Online]. Available: http://www.growthbusiness.co.uk/biometrics-in-business-18454/. [Accessed 2 October 2016].

[19] C. R. Wright, "Human Resource Executive Online," 18 December 2014. [Online]. Available: http://www.hreonline.com/HRE/view/story.jhtml?id=534358112. [Accessed 6 October 2016].

[20] P. Salil, P. Sharath and Anil.K.Jain, "Biometric Recognition: Security and Privacy Concerns," IEEE Computer Society, 2003.