Chapter 7

On Biometrics and Profiling: A Challenge for Privacy and Democracy?

Daniele Cantore
University of Pavia, Italy

ABSTRACT

This paper advances an analysis of biometrics and profiling. Biometrics represents the most effective technology in order to prove someone's identity. Profiling regards the capability of collecting and organizing individuals' preferences and attitudes as consumers and costumers. Moreover, biometrics is already used in order to gather and manage biological and behavioral data and this tendency may increase in Ambient Intelligence context. Therefore, dealing with individuals' data, both biometrics and profiling have to tackle many ethical issues related to privacy on one hand and democracy on the other. After a brief introduction, the author introduces biometrics, exploring its methodology and applications. The following section focuses on profiling both in public and private sector. The last section analyzes those issues concerning privacy and democracy, within also the Ambient Intelligence.

1. INTRODUCTION

In every society, owning the information means being able to handle a situation. This becomes especially preeminent if dealing with complex societies where the fragmentation of information gives more leverage to whom is able to manage that information. In our technological world, one of the most challenging problems refers to the increasing data overload. Therefore, it has become essential to be able to discriminate useful information from useless information.

Profiling activities allow public administration and private corporations to sharpen their aims becoming more effective in achieving their goals and purposes. As a matter of fact, profiling allows gathering and organizing individuals' data. In particular, within the public sphere, profiling is used in order to increase safety and law enforcement; in private business, it regards the capabilities of knowing stakeholders' attitudes and interests in order to make more effective marketing and com-
munication campaigns. However, due to the fact that profiling regards individuals and their data, the process of collecting and managing those data can never be considered neutral.

In this paper, I will describe the importance of profiling techniques in our contemporary society, both in public and private applications, especially as they are related to biometrics. First of all, I will describe biometrics and its procedures as an example of technology that is used in forensic and other law-enforcement applications. I will then explore some methodologies, used to profile people, that benefit private businesses including individual profiling and user profiling on the one hand, and distributive profiling and non-distributive profiling on the other. Successively, I will explore some of the possible issues regarding biometrics and profiling within the paradigm of Ambient Intelligence (AmI). Through this paper, I will stress the actual necessity of creating a law-system able to cope with profiling, also foreseeing future developments and issues. At the same time, I will attempt to shed light on some aspects strictly related to our current concepts of democracy, technological development, and violence, especially focusing on privacy issues within biometrics and the AmI context.

The basic idea throughout this paper is to create a framework where those topics are juxtaposed rather than analysing them one by one. This way, I hope to show the complexity of these themes and how profoundly intertwined they are.

2. INTRODUCING BIOMETRICS: METHODOLOGIES AND APPLICATION

Biometrics regards the possibility of recognizing someone’s identity from an unambiguous set of biological data, or behaviour. The essential idea is that every human being is unique: no matter how many physiological features or feelings or behaviours all human beings have in common, every person is different one from others just like every snowflake is different from others. Biometrics techniques can be divided and categorized in two different areas: (i) physiological: including DNA, facial-scan, finger-scan, hand-scan, iris-scan, otoacoustic emission, retinal-scan, vascular patterns; (ii) behavioural: including gait, gesture and grip, handwriting, keystroke, lip motion, mouse movements, signature, voice. Obviously, each of those techniques has reached a different level of maturity. Nevertheless, they have all developed for two different ends: (i) to protect information: especially biological data are detected in order to replace old systems based on passwords or PINs for identification purposes; (ii) to perform various kinds of verification: biological data are detected in order to assess someone’s identity, especially in forensic applications for verification purposes.

In order to shed light on biometrics in a more specific way, it is essential to clarify and distinguish the areas in which it operates starting from the difference between identifying someone and verifying someone’s identification: (i) identifying means to establish that a particular person, thing or quality corresponds to a determinate identity; (ii) verifying one’s identity is about assessing the validity and truthfulness of the relationship I just defined. As for biometrics, the different meaning between these two words shows the differences in their applications: (i) the first case refers to those determining criteria used to establish the identity of a certain person; (ii) the second case refers to the necessity of a verification process that allows the adoption of evaluation criteria to approve the legitimacy of an individual’s request, and consequently allow her to access a certain system (Nanavati, Thieme, & Nanavati, 2002).

In the identification system, the methodology involves searching a database containing the biometric data of many people in order to find a match with one of them. This type of activity is known as one-to-many matching, and it is often used in the forensic domain, especially to apprehend wanted people by using watch-lists. The identification