Chapter 12
Ethics and Policy of Biometrics

Emilio Mordini

Abstract This chapter describes the ethical and privacy implications concerning biometric technology. Two emerging issues related to biometrics, function creep and informatization of the body, are discussed. Because function creep results from the over-generation of data, the argument is made that, by design, biometric applications are unlikely to cease the collection and processing of surplus amounts of personal data. Concerning informatization of the body, biometrics can be seen in both a positive and a negative light. When biometric technology is used to give a personal identity to a previously unidentified person, an increased sense of personal empowerment through the attainment of identity is witnessed. However, when biometrics is instead used to offer an identity to individuals solely for the purpose of categorization, we can then consider this to be an unwelcome risk of this technology. Thus, care must be taken in the application of biometric technology.

12.1 Introduction

Scientific literature on ethical and privacy implications of biometrics is becoming increasingly important. A sharp debate is emerging about whether biometric technology offers society any significant advantages over conventional forms of identification and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian governments. Main issues at stakes concern large-scale applications, biometric databases, remote and covert biometrics, respect for fair information principles, medical applications, enrolment of vulnerable and disabled groups, information sharing and system interoperability, technology convergence and behavioural biometrics surveillance. It is, however, arguable as to whether it makes sense to discuss all these issues together without differentiating between different biometrics and applications. As a matter of fact, biometrics encompasses so many different technologies and applications that it is hardly thinkable to develop arguments which are valid in all circumstances. Yet there are two interrelated issues
about biometrics that are worth discussing in general terms. They are “function creep” and the so-called “informatization of the body”.

12.2 Function Creep

“Function creep” is the term used to describe the expansion of a process or system, where data collected for one specific purpose are subsequently used for another unintended or unauthorized purpose. Since 2001, function creep has been in the limelight of the ethical and privacy debate [29]. Function creep represents a serious breach of the ethical tenet that requires a moral agent to be honest and responsible for her actions; from a political perspective function creep is a serious lesion of public trust and menaces to destroy confidence in biometric systems. Most problems connected with respect to privacy and data protection in biometric applications are actually rooted in the issue of function creep.

Generally speaking, function creep refers to information that is collected for one purpose but being used for another. Consequently, in the context of biometric identification it should refer to any use of biometric data different from mere identification. Function creep in the field of automated personal recognition may be motivated by several reasons (from state intelligence to commercial purposes) and it is not limited to biometric identification. Most examples of function creep are indeed rather innocuous. The “Social Security Number” in the United States is an often cited example of function creep. Although the original social security cards bore the warning that the SSN could not be used for identification, in the 1960s the Internal Revenue Service started using the SSN for tax payer identification and today the SSN has been the main identity document used by most US citizens. Function creep usually involves three elements: (1) a policy vacuum; (2) an unsatisfied demand for a given function; and (3) a slippery slope effect, or a covert application. A policy vacuum is probably the most important element to determine the risk of function creep. When organizations (be it small companies, large industries, or governmental agencies) adopt new information technologies, or new information schemes, failing to create specific policies, these technologies end up being driven only by the different interests of various stakeholders. As a result, the new scheme may develop in a quite different sense – sometimes even opposite – from that primarily intended. Civil liberties advocates have the tendency to implicitly blame people because they adopt new technologies without considering the downside. Yet it is evident that the main responsibility rests with policy makers who should create the opportune policy frame for innovations.

An unsatisfied demand for a given function is the second important element that has the potential for creating a function creep. Information collected for one purpose is used for another when there is a need that is not properly met. In the example of the SSN, it is evident that the lack of a suitable tax payer identifier was the main driver for the SSN’s mission change.

Finally, function creep must develop almost unnoticed. Usually, function creep happens for one of two reasons: either the new functions develop little by little,