IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com

ITB15305

This chapter appears in the book, ***Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions*** by **R. Subramanian** © 2008, IGI Global

Chapter VI

Rational Concerns about Biometric Technology: Security and Privacy

Yue Liu, University of Oslo, Norway

Abstract

The increasing use of biometric technology is often accompanied by grandiose claims about its ability to enhance security and the debate over the perceived threats that it poses to the notion of privacy. By focusing on the security and privacy concerns the biometric technology raises, this chapter gives critical analysis on the complexities involved through rational discussions, technology assessment and case examples. It clarifies the prevalent misconceptions concerning the biometric technology and finds that biometric technology alone can not provide an answer to security issues. The inherent nature of biometric technology provides enormous potential for undermining privacy. However, security and privacy are not necessarily two contradictory concepts where biometrics is concerned.

Introduction

Across the various contexts in which it is applied, **biometric technology** (hereinafter also termed "biometrics") raises multiple **rational** concerns. This chapter aims to give some idea of the complexities involved in biometric technology by focusing on the **security** and **privacy** concerns it raises. To what extent do and will biometrics affect privacy and security? Exactly what is the special nature of biometric data compared with other personal data? Is the increasing use of biometrics just a question of "balance" or "trade-off" between privacy and security? It is with these sorts of questions that this chapter is concerned. In tackling such questions, the chapter also aims to clarify some of the misconceptions that inform parts of the legal discourse around biometrics.

Background

Put simply, biometric technology involves the use of automated methods for verifying or recognizing the identity of a living person based on their physiological or behavioral characteristics.[1] Most people get to know about biometrics from what they observe in science-fiction movies like Spielberg's *Minority Report*, in which people are regularly subjected to eye scans for identification, control, and/or advertising purposes when they take public transport, enter office buildings, or simply walk in the street. Seductive claims also have been made about the ability of biometrics to defeat terrorism and organized crime. Biometrics figure increasingly as the centerpiece technology in implementing counterterrorist policy.

Much technology inspires not only hope but also fears, and development of innovative technology has almost always raised new legal concerns. This is certainly true in the case of biometric technology. Increasing use of biometrics has led to fears of an acceleration in the speed at which our society becomes a surveillance society with scant room for personal privacy and autonomy. Doubts also have been raised about the level of security that increased use of biometrics can actually deliver. It further is feared that the loss of privacy may lead in turn to a host of other problems, such as increasing social stigma, discrimination in employment, barriers to gaining health insurance and the like. With the growing use of biometrics, it is of paramount importance that discussions about the ethical, social, and legal implications of the technology take place. In such discussions so far, privacy and security concerns often have figured prominently[2]—and for good reason, as this chapter highlights.