# Chapter V
# An Extension of the Technology Acceptance Model to Determine the Intention to Use Biometric Devices

**Tabitha James**
*Virginia Polytechnic Institute and State University, USA*

**Taner Pirim**
*Mississippi Center for Supercomputing Research, USA*

**Katherine Boswell**
*University of Louisiana - Monroe, USA*

**Brian Reithel**
*University of Mississippi, USA*

**Reza Barkhi**
*Virginia Polytechnic Institute and State University, USA*

## ABSTRACT

*Protection of physical assets and digital information is of growing importance to society. The need for development and use of security technologies is ever increasing. As with any new technology, user acceptance of new software and hardware devices is often hard to gauge, and policies to introduce and ensure adequate and correct usage of such technologies are often lacking. Security technologies have widespread applicability to different organizational contexts that may present unusual and varied adoption considerations. This study adapts the technology acceptance model and extends it to study the*

*intention to use security devices, more specifically biometrics, across a wide variety of organizational contexts. Due to the use of physiological characteristics, biometrics present unique adoption concerns. The extension of the technology acceptance model for biometrics is useful, as biometrics encompass many of the same adoption concerns as traditional security devices, but include a level of invasiveness that is obvious to the user. Through the use of vignettes, this study encompasses a systematically varied set of usage contexts for biometric devices to provide a generalizable view of the factors impacting intention to use over all categories of situational contexts of the device's use. The technology acceptance model is extended in this study to include constructs for perceived need for privacy, perceived need for security, and perceived physical invasiveness of biometric devices as factors that influence intention to use. The model is shown to be a good predictor of intention to use biometric devices and implications of the results for biometric and security technology acceptance is discussed.*

## INTRODUCTION

Property theft, violent crimes, theft, and misuse of digital information, terrorism, and threats to privacy, including identity fraud, in today's digitally connected, mobile society necessitate the development of tools to protect digital information and physical assets by both individuals and corporate entities. According to findings from the National Crime Victimization Survey, approximately 23 million U.S. residents were victims of crime in 2005, including both property crime and violent criminal acts (Bureau of Justice, 2005). The 2006 CSI/FBI Computer Crime and Security Survey reported that 52% of their participants reported unauthorized computer use. Out of the respondents that were willing or could quantify the financial implications, the amount of losses reported exceeded $52 million (Gordon, Loeb, Lucyshyn, & Richardson, 2006). The Federal Trade Commission reported 246,035 identity theft complaints in 2006 which accounted for 36% of all FTC complaints for the year (Federal Trade Commission, 2007). The most common form of identity theft reported was credit card fraud which accounted for 25% of the complaints, followed by phone or utilities fraud, bank fraud, and employment fraud (Federal Trade Commission, 2007).

The need to secure both digital and physical assets is apparent from these statistics, yet it is often difficult for technology to keep pace with the growing number of threats and the increasing number of vulnerabilities that exist in traditional methods of security. A method of identification that has been growing in popularity is the use of physical or behavioral traits, such as fingerprints or DNA, to identify and authenticate individuals. Certain physical and behavioral traits are unique to each individual and therefore may provide methods of identification that are more successful than traditional approaches. Technological devices that utilize these unique traits to identify and authenticate an individual are known as biometrics. These devices have the obvious advantage of not falling prey to many of the well known vulnerabilities of traditional methods. Since a biometric device uses a unique biological trait to distinguish an individual, it is very difficult and often impossible for the identifier to be lost, stolen, duplicated, or given away (Liu & Silverman, 2001). This advantage makes biometric devices an appealing option for individuals and corporations that wish to adopt a new security technology.

The technology acceptance model (TAM) has received wide acceptance for studying the usage behavior of new technologies (Davis, 1989). We extend TAM to determine the intention to use security technologies, specifically biometric devices. We utilize a vignette based survey design to study the user behavior towards biometrics and the intention to use these devices. This approach provides a general overview of individual's per-