



## **Biometric Use Cases: Choosing the Right Biometric for the Job**

*Speaker Verification has received short shrift from security mavens, largely because it has been ill-positioned by the speech processing community and has been subject to misplaced concern over its relative "strength" compared with more expensive, hardware-intensive alternatives. In this report, Opus Research assesses the comparative strengths and weaknesses of four major biometrics: facial, fingerprint, iris and voice. Also presented are appropriate use cases for each biometric technique, including a case study of a working governmental Speaker Verification system.*

**November 2005**

**Avery Glasser  
Analyst**

**Case Study provided by Opus Research Associate  
Dr. Clive Summerfield  
Adjunct Professor, University of Canberra**

Opus Research, Inc.  
330 Townsend St., Suite 201  
San Francisco, CA 94107

---

For sales inquiries please e-mail [info@opusresearch.net](mailto:info@opusresearch.net) or call +1(415)904-7666  
This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believed to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.

Published November 2005. © Opus Research, Inc. All rights reserved.

## Key Findings

- People employ rudimentary biometric identification and verification techniques on a daily basis, illustrating the rich variety of modalities and security levels.
- There are fundamental differences between identification and verification, each requires different levels of security and solves different business concerns.
- Voice is a “behavioral” biometric, whereas fingerprints, facial and iris patterns are “physical” in nature. Physical biometrics present the problem of determining if a claimant is aware, cooperative or even alive at time of authentication.
- A key advantage of the use of voice biometrics for speaker verification is that there is no need for specialized or dedicated hardware. This has significant financial impact for mass deployments across broad geographic regions
- Existing research results demonstrate that the False Acceptance and False Rejection Rates of voice biometrics meet or exceed fingerprint, iris and facial scanning when applied appropriately. For large scale enterprise and government deployments, speaker verification presents a highly cost-effective, scalable approach

## Table of Contents

Key Findings .....	ii
Table of Contents .....	iii
Picking the Appropriate Biometric.....	2
The First Biometric Readers.....	2
Verification versus Identification .....	3
Signing a Receipt Answers the Challenge .....	3
Working without Claimed ID .....	3
Manual Processes Scale with Automated.....	4
Automation Promotes Scale and Accuracy.....	4
Physical and Behavioral Biometrics .....	5
Centralizing Biometric Resources.....	6
Active versus Passive Identification .....	7
Market Projection for Biometrics.....	7
Technology Assessment: Fingerprint.....	8
Technology Assessment: Facial .....	9
Technology Assessment: Iris .....	10
Technology Assessment: Voice .....	11
Use Cases for Selected Biometric Methods .....	13
Case Study: Voice Biometrics and the Australian Government.....	14

**FOR SALES INQUIRES CONTACT US AT  
1-415-904-7666 or [info@opusresearch.net](mailto:info@opusresearch.net)**