BIOMETRIC RESEARCH AGENDA

REPORT OF THE NSF WORKSHOP

Editors: Edwin P. Rood and Anil K. Jain
Edwin.Rood@mail.wvu.edu ; jain@cse.msu.edu
304-293-8281

April 29 – May 2, 2003
Lakeview Scanticon Conference Center
Morgantown, West Virginia

Organizers: Ruud M. Bolle, IBM Research
Anil K. Jain, Michigan State University
Jonathon Phillips, DARPA
Edwin P. Rood, West Virginia University
Jim Wayman, San Jose State University
John D. Woodward, RAND

Released July 1, 2003

NSF Grant # EIA-0240689

Program Director:
Dr. Gary Strong
Experimental and Integrative Activities
Directorate for Computer and Information Science and Engineering
National Science Foundation

TABLE OF CONTENTS

Executive Summary

Overview

The *Workshop for a Biometric Research Agenda* was convened in Morgantown, WV from April 29 through May 2, 2003 to develop a rational and practical description of crucial scholarly research to support the development of biometric systems for human verification and identification. Fifty-five experts from academia, government, and industry participated in the by-invitation-only Workshop. The participants deliberated on crucial research needs in the areas of technologies, measures of effectiveness, societal and political implications, and economics and workforce. This Workshop was the first gathering of many of the international leaders in biometric research for the specific purpose of creating a research agenda. Key research areas were identified, and an attempt was made to prioritize the needed research. The highest priority was given to the development of statistical models for biometric verification, identification, and scaling of databases. Additional outcomes from the Workshop included the acknowledgement that research in different technologies, or biometric modalities, use different esoteric languages, and there is a need for further interactions among the research communities to share results of discovery at the fundamental level. This research agenda is the first attempt for the field of biometrics at such a broad scale, and should be considered a living document to be refined and matured at future biometric conferences and workshops. For example, specific research areas including political implications and workforce development, and to some extent public outreach, remain without defined research agendas.

Workshop Goal and Objectives

The goal of this workshop was to develop a consensus for a biometric research agenda by convening national and international experts for this sole purpose. The experts represented the various disciplines that collectively define the field of biometrics. These disciplines include natural science and engineering, as well as social science, political science, economics, and other disciplines. Considerable preparation and follow-up were required for this "first of its kind" workshop. Activities included 1) forming an Organizing Committee responsible for directing the workshop, 2) identifying the national and international experts who should be invited to the workshop, 3) working with those experts prior to the convening of the workshop to develop an agenda and discussion items, 4) writing the workshop findings in the form of a report, and 5) presenting the findings to the NSF and disseminating them to the scientific community. These goals and objectives were met.

Research Drivers

The principal need for this workshop is that the United States has yet to develop a long-range biometric research agenda to fulfill anticipated technology requirements to meet stringent performance requirements, and to develop a knowledge base to support statistical analysis of biometrics and public administration of biometric policy. Current deployment of biometric systems is largely vendor-driven, and there is a need to conduct research to understand and formally evaluate the dynamics of biometric systems in our society.

The workshop was intended to address the following research issues:

(1) What biometric **technologies** are currently deployed, currently available but not yet deployed, and in development that could be deployed in the foreseeable future?
(2) What **measures of effectiveness** are required to ensure that these technologies help to provide higher levels of security?

(3) What are the **societal and political implications** of biometric technologies for personal security and preservation of individual liberties, and for lifestyle within our society?
(4) What are the **economic** versus effectiveness trade-offs in implementing these technologies, and the impact on productivity, and how is a **workforce** created?

During the planning stages and early in the Workshop, the consensus was reached that this list of issues needed some modifications to place more emphasis on understanding biometric systems, and less emphasis on futuristic technologies. Therefore, the questions addressed at the Workshop were modified to the following:

1) What measures of effectiveness should be used for the evaluation of recognition performance of biometric technologies?
2) What research is required to determine the potential societal, legal, and political implications of these technologies?
3) What research is required to determine the cost effectiveness and economic impacts of these technologies?

Research Agenda Highlights

The major finding of the Workshop is that there is a critical need to understand and exploit existing biometric technologies with respect to modeling and scaling, quality of biometric data, fusion of modality and results, and system performance. The research agenda focuses on items that provide cross-cutting knowledge across technologies even if investigated in the context of a specific technology. There is a need to develop a statistical understanding of biometric systems sufficient to produce models useful for performance evaluation and prediction. Public perception, consumer reaction, ergonomics, and habituation are important research agenda items underlying public acceptance of biometric technology. Privacy agenda items revolve around notions of "privacy enhancing" and "privacy invasive" perspectives, and agenda items include developing the relevant and most significant questions to be addressed in terms of meaningful implementation of biometric technology. Economic agenda items include developing metrics that are appropriate to biometric systems that by nature may have far-reaching impact on user behavior and business cost.

Background

The need for the Workshop was suggested by the proceedings of the recent Biometrics Consortium Conference (BC2002) held in September 2002, in Washington, DC. The annual Biometric Consortium Conference provides a forum for government and other users, system developers and other vendors, and to some extent academic researchers, to exchange information on the state-of-the-art in biometrics. Although biometric systems have been deployed extensively over the past 30 years, the results appear mixed perhaps because of an inadequate knowledge base upon which biometric technology can be evaluated and advanced. This observation, which was the original impetus for establishing the Biometric Consortium in 1992, led to this Workshop in an effort to identify a research agenda that would address cross-cutting issues such as rigorous methodologies for measuring statistical effectiveness and implementing biometrics in society at large.

Biometrics is a multidisciplinary field best described as a convergence of traditional disciplines. This Workshop was constructed to encourage interactions between researchers investigating the

different aspects of biometrics. The emphasis was on treating biometrics as a unified field in which engineers, computer scientists, sociologists, and lawyers collectively addressed the research issues.

Following BC2002, coprincipal investigators Edwin Rood and Anil Jain approached the National Science Foundation to obtain support for this workshop. The NSF by statute is authorized to support science and engineering activities relating to national security, and to provide a service to the federal government as well as the research community, NSF supported this workshop.

Current Research Endeavors

An overview of the current biometric research activity worldwide would show an emphasis on field application of proprietary biometric systems, and a corresponding focus on developing standards mostly for interoperability with respect to data exchange. There are numerous conferences worldwide, but most of them focus on exhibits and applications, such as case studies for which the performance outcomes are presented or surmised. The academic conferences are traditionally divided along technology lines. For example, speaker recognition work is generally reported at the International Conference on Acoustics, Speech and Signal Processing, while facial recognition work is presented at, for example, the International Conference on Computer Vision. Similarly, scholarly journals are also divided primarily by technology, or biometric modality.. The Federal investment in university research directly for biometrics is relatively small, perhaps on the order of $10M a year currently. This Workshop identified and produced a biometric research agenda targeted at the crucial issues underlying advances in technology (or biometric modality), measures of recognition effectiveness, societal and political implications, and economics and workforce.

Organization of the Workshop

The Organizing Committee consisted of six persons: the two coprincipal investigators, Edwin Rood and Anil Jain, who also served as cochairpersons for the Workshop, and four additional persons (Ruud Bolle, IBM Research; Jonathon Phillips, DARPA; Jim Wayman, San Jose State University; and John Woodward, RAND). This Committee, consisting of academic, government, and industry representatives well known to the international biometric research community, performed the selection and invitation of participants. The participants were assigned to Working Groups corresponding to three research issues, as shown in Table 1. Note that although the Workshop identified a total of four research issues, two of those issues were combined with the result that there were only three working groups. In addition, invited keynote speakers gave presentations to the whole Workshop as shown in the agenda in Table 2. The agenda further shows how the working groups met separately and as a "whole" to produce an integrated cross-cutting research agenda.

The Workshop produced the research agenda required to meet anticipated biometric system needs. The Workshop did not specifically address the state-of-the-art for biometrics as a prelude to discussion of the research agenda. Because the participants were selected based on their peer-recognized expertise on the state-of-the-art, the Workshop discussions directly addressed the research agenda. Accurate resources for assessing the state-of-the-art in current biometric deployments are sparse, as was discovered by the General Accounting Office last year as reported in the 2002 paper "Technology Assessment: Using Biometrics for Border Security" (GAO-03-

174), on-line at http://www.gao.gov/new.items/d03174.pdf . The book *Biometrics: Personal Identification in Networked Society* (Kluwer Academic, 1999) is recommended reading for a scientific overview of the state of biometrics. A general overview of the subject is presented in the book *Biometrics* (McGraw-Hill, 2003) and *Guide to Biometrics: Selection and System Design* (Springer, 2003).

The immediate results from the Workshop were developed into a draft report by the Organizing Committee, and distributed to the participants for comments. This report represents the consensus findings of the Workshop. This report is presented to the NSF for further comments, and will be discussed in open forum at the Biometrics Symposium as part of the Biometrics Consortium Conference (BC2003) in Washington DC, in September 2003. Additional comments from that peer discussion will be reviewed by the Organizing Committee and incorporated into this report as appropriate.

Research Agenda

The findings of the Workshop and the proposed research agenda are listed according to the four research issues: technologies, measures of effectiveness, societal and political implications, and economics and workforce. Some research items are relevant to more than one issue, and in those cases the item was usually arbitrarily related to only one of the issues. On occasion there is overlap between items listed in the four different research issues, but this could not be avoided. By definition, biometrics is multidisciplinary and the research issues are intertwined. In some respects, the presentation of the Workshop findings develops taxonomy for biometric research.

As noted earlier, the research agenda presented here to the National Science Foundation is a draft report, to be updated at the conclusion of the Biometrics Symposium in September 2003. Although developed by a number of leading experts, the agenda reflects the status of an emerging field of science and technology. As such, this agenda provides direction for the research community and should be viewed as a living document.

The priorities for the research agenda are described in the section Research Priorities. The more comprehensive lists below are the significant items for an agenda, and are presented according to the four research issues.

Technologies

Recommendations for research agenda items are arranged according to the cross-cutting items, and then each of the major technologies, or biometric modalities: fingerprints, face recognition, iris pattern, and speech. The most widespread technology in terms of the number of deployed units is perhaps hand geometry, but because the approach is proprietary, it is not included here. No additional biometrics such as gait, retina, optical skin reflectance, or chemosignals were listed for future exploitation. The consensus was that existing technologies have much to be understood and to be exploited before moving into less-known technologies. The expectation is that results from basic research on traditional technologies will be transferable to future technologies.

Cross-Cutting Items

1. Template Aging – short term, long term temporal changes in the biometric template

2. Fusion, including the weighting of different information sources for the purpose of increased recognition performance
    a. Multimodal methods – measurements of multiple biometric characteristics (for example fingerprint added to hand geometry)
    b. Concurrent and sequential decision-making for fusion
    c. Acquisition and maintenance of multimodal sample databases
    d. Fusion algorithms for different biometric modalities using these databases
    e. Algorithms – integrating results from algorithms applied to the same database
3. Modeling and scaling
    a. Understanding of error probabilities and correlations between different biometric modalities
    b. Probabilistic system error modeling and error statistic estimation from correlated samples
    c. Statistical prediction of operational performance from laboratory testing
    d. Prediction of large database identification performance from small-scale performance
4. Quality of biometric data
    a. Relating biometric sampling quality to performance improvement
    b. Distinctiveness – parametric and statistical modeling of the biometric modalities to study how they distinguish persons absolutely
    c. Standardization of data collection to ensure quality; determine meaningful metrics for quality
5. System performance
    a. Modeling the matching process as a parameterized system accounting for all the variables
        i. Determine the best payoff for system performance improvement
        ii. Tuning and training the system parameters
    b. Statistical modeling and measurement of the recognition processes
    c. Effect of biometric error conditions and failures on system performance
        i. Alternate biometric modalities for exception handling
        ii. Modeling the throughput of verification and identification systems
    d. Ergonomic design of the capture system and usability studies
    e. Convenience and intuitiveness of the user interfaces
    f. Methodology for arriving at quantitative level of performance such as bit strength for different biometric modalities (e.g., comparison to four-digit pin)

Face Recognition

1. Facial image acquisition with different pose and lighting
    a. Account for variations in illumination and viewing conditions, such as outdoor conditions
    b. Utilize photographs from uncontrolled conditions
2. Template aging as a particular issue for facial recognition
    a. Development of synthetic face aging techniques
    b. Database development (over time) for purpose of compensating for aging
3. Understand how the human visual system recognizes faces
4. Capitalize on commonality of signals for face and voice
5. Fusing of signals for face and voice for increasing recognition performance

Fingerprint Matching

1. Establish the optimal resolution for fingerprint image acquisition
2. Fundamental mathematical understanding of minutiae and feature extraction for matching and indexing
3. Develop optimal approaches to combining various types of fingerprint characteristics (e.g., pattern data, minutia, level 3 detail, etc.) for more effective matching
4. Increased recognition performance using multiple samples from multiple fingers
5. Investigate the potential for sensing multiple types of biometric data from a finger (e.g., thermal profile, optical dispersion profile, etc.) to be used in conjunction with the friction ridge pattern for multimodal biometric matching

Iris Recognition

1. Determine the recognition performance limits of iris scanning
    a. Iris image acquisition under unconstrained conditions
    b. International collaboration with China and Russia
2. Extend the operational performance envelope to include suboptimal imaging conditions
3. Probabilistic and anatomical study of theoretical limits
4. Study of image comparison techniques for iris recognition
5. Extraction and reconstruction of iris images from face images

Voice Recognition

1. Investigate recognition performance with noncooperative subjects
2. Study voice signal cross-channel variability (microphone, handset, compression, transmission line changes)
3. Better physiological and linguistical understanding of how a person speaks
    a. Ideolects (e.g., word usage)
4. Generalized norming in the speaker community
5. Capitalize on commonality of signals for face and voice

<u>Measures of Effectiveness</u>

The research agenda for measures of biometric effectiveness addresses the items necessary to support biometric technology development, statistical system comparison and performance prediction. The impact of public perception was also included.

Fundamentals

1. Study the theoretical limits of recognition performance for:
    a. Face
    b. Finger
    c. Iris
    d. Speech
    e. Integrated multimodal biometrics

2. Establish statistical models and theories for system performance comparisons and performance predictions
    a. Methods for summarizing large amounts of data into a small set of numbers reflecting the statistical essence of the data
    b. Rank order statistics versus trade-off errors (receiver operating curves)
    c. Design and acquisition of biometric databases (sampling design)

Technical Performance

1. Distinguish between technology, scenario, and operational evaluations:
    a. Sample size issues and uncertainty in estimates, confidence intervals
        i. Non-independent non-identically distributed samples
        ii. Do the evaluations vary by technology and/or application?
    b. Operational test protocols for error condition simulation
2. Determine statistical models and theories that are most compatible for these performance evaluations
    a. Do new metrics/statistics need to be developed?
        i. Extreme value statistics to understand very small error rates
        ii. Fusion of modern statistics with machine learning and pattern recognition
    b. Assess the need for application and technology dependent metrics and procedures
    c. Harmonization to provide common procedures and interchangeability
3. Determine procedures for evaluations
    a. How to best implement pre- and postprocessing of the evaluation data
4. Develop statistical comparisons of the evaluation results
    a. Meta-analysis utilizing information collected for unplanned statistical analysis
    b. Development of measurements for biometric data quality
    c. Blind evaluation versus preprocessing and postprocessing of the data
5. Determine the theoretical limits of measurement accuracies for a given database (confidence intervals)
6. Statistical projection and estimation of operational recognition performance from empirical data
7. Study the measurement stability of recognition performance metrics
    a. Different subject groupings
    b. For the same subject with different sample acquisition conditions and acquisition times
    c. Different metrics for the same data
8. Data and “meta-data” quality assessment and control (planned and unplanned statistical analysis)
9. Is “one standard, one test, one report for each biometric system” a desirable, feasible goal?

Integration of Measures of Effectiveness

1. How to combine different biometric modalities given correlated biometric data samples
2. Biometric data fusion algorithms without the use of prior probabilities of imposter and genuine subjects
3. Develop methods for inclusion of prior information and costs into biometric system design

4. Study the scalability of large identification systems
    a. Can you test scaling behavior without using large-scale databases?
5. Collect open benchmark datasets with sequestered components to improve test and evaluation process

Data Collection, Documentation and Storage

Model after the DARRPA-NIST Linguistic Data Consortium (LDC)

1. Open data sets for developers
2. Sequestered data sets for testers
3. Additional modalities and meta-data (meta-data as opposed to the biometric corpus)
4. "Slaps" (four finger impressions from one placement)
5. Iris image databases
    a. Make available to research community a database of systematically documented iris images.
    b. Should include cases that are designed to tax current recognition approaches
    c. Build on preliminary data available from the DARPA HumanID Program and the Chinese Academy of Sciences
6. Large-scale multimodal databases
7. Linking data sets
8. Usability/repeatability

System and Interoperability

1. Boundary identification and interfaces
    a. Varies by application
        i. E.g., Wiegand distribution for access control
    b. Develop compliance test procedures
    c. Using performance measures for biometric system components
        i. Obtaining recognition performance estimates of the entire system from component measure estimates
2. Application of glass box complex system for testing (modular component testing for the purpose of large-scale system performance prediction)
3. Modeling and measuring of system throughputs
    a. How application-dependent is this?
    b. How do you measure throughput for the biometric module in the system, the system itself, or the system including human interaction?
    c. Study throughput tradeoffs with processing time, bandwidth, and accuracy
    d. Determine throughput effects attributed to habituation

Consumer Reaction and Public Perception

1. Determine the impact on recognition performance of
    a. General public knowledge of biometric technology
    b. Understanding of the application
    c. Understanding of the technology

2. Understand the impact of perceived error rates on prior probabilities of genuine and imposter subjects
3. Understand the habituation patterns of different user populations with different technologies and product implementations
4. Determine the incentive threshold behavior of different user groups with different technologies, products and applications

Societal and Political Implications

Agenda items address public acceptance of biometrics and public administration of biometric policy. Public acceptance of biometric technology may lead to effective implementation of procedures for ensure one person – one identity.

Political Implications, Civil Liberties, and Law

1. Under what conditions does biometrics have a positive or negative impact on privacy?
2. Under what conditions will biometrics serve as a Privacy Enhancing Technology (PET) or Privacy Invasive Technology (PIT)?
    a. PET-Suggested research topics: Do/can biometrics lead to
        i. Identity theft prevention/deterrence/recovery?
        ii. Minimization of secondary information collection?
        iii. "Anonymous biometrics," the capability of removing (hiding) the true identity from the biometric?
    b. PIT-Suggested research topics: Do/can biometrics lead to
        i. Invasion of "personal space"?
        ii. Reduction of anonymity?
        iii. Big Brother/Little Brother (loss of control of personal information)?
3. Should privacy policies for biometrics be promulgated?
    a. If so, what are the principles?
    b. If so, by whom?
        i. Legal institutions
            1) Privacy laws and regulations
            2) Other enabling laws and regulations
                a) E.g., Daubert ruling (court acceptance of science)
                b) Legal "signature"
        ii. Technical standards community

Human Factors (Usability and Accessibility)

Human Factors directly impact error rates, and error rates directly impact the perceived recognition performance of the system.

1. Establish a range of subject characteristics that can be used to evaluate user metrics for each biometric
2. Determine the adaptive range of sensors to deal with the subject characteristics?
3. Failure-to-acquire and failure-to-enroll are roadblocks for usability; what are the user issues in addition to the technical issues?

4. Given that usability must be considered for both the subject and the operator, what measurements must be made of the trade-offs such as FNMR vs. FTE, FNMR vs. number of attempts, FNMR vs. number of modalities (system complexity), FNMR vs. perceived FMR (introduction of priors), and level of supervision vs. error rates?

Security of Biometric Applications and Systems

1. How much confidence does/should society have in existing security systems?
2. How much confidence does/should society have in biometrics systems?
    a. How secure are systems perceived to be?
    b. Are concerns security-based or error-based?
    c. What are the misconceptions, and how can they be addressed?
3. Is it feasible to develop a structure for classifying vulnerabilities, types of attacks, etc. for biometric systems?
    a. Populate standard threat structure with biometric-specific factors, and proper responses.
4. Determine how to measure "perception cost" vs. perception benefits, and assess, quantify and predict public perception

Enrollment and Data Management Issues

1. What is/should be needed to establish an identity?
    a. Are there weak links? What are they? Can biometrics help?
    b. Can reliability of breeder-documents (identity creation) be improved? How?
    c. Do people have an unrealistic belief in the current method of establishing identity?
2. Is there a difference between societal acceptance of identification and verification?
    a. If yes, is the difference limited to concerns about a central repository?
        i. What other concerns are there?
    b. How can the concern about central databases be reduced?
3. What factors apply to unsupervised enrollment?
    a. Use of biometrics for convenience rather than security

Scope and Scalability Issues

1. What are the implications of the following on usability, cost, acceptance, etc.?
    a. Mandatory vs. voluntary use
    b. Standards
    c. Citizenship of subjects
    d. Public vs. private-sector use
    e. Linking children to an identity
        i. Visa issuance
    f. Interchange of information among local, state, federal, and tribal governments and agencies
2. How do you ensure adequate, available data (with meta-data) for test & evaluation?
3. Should the data be public or sequestered?

Economics and Workforce

Agenda items address both the cost of deployment, and the consequences of this cost.

Costs and Benefits of a Biometric System

1. What are the ongoing costs/benefits of existing systems?
    a. How do you measure and model these, to include secondary costs of an existing system, such as fraud and identity theft?
2. How do you measure and quantify the benefits that biometrics would add?
    a. What secondary effects or loopholes would be caused by the deployment of biometric systems?
        i. What secondary benefits (of existing systems) would be removed? For example:
            1.) Purposeful loan of a password or PIN
            2.) Anonymity
    b. How do you measure deterrence effects?
    c. How do you measure the benefit of avoiding rare events (such as 9/11)?

Measures of Effectiveness for Economic Impacts

1. How to measure the fiscal cost of a biometric system?
2. How to measure the fiscal cost of existing/alternative systems?
3. How to measure enhancement of system upgrade versus existing/alternative systems?
4. How do you compare costs and benefits?

Conclusions and Other Findings

In the process of developing the research agenda, the Workshop produced discussions that led to findings that are listed here in the interest of furthering understanding of the emerging field of biometrics in the scientific community.

1. There is evident need for the biometrics research community to interact among technologies (biometric modalities) as well as among research issues.
2. Biometrics is both a traditional field of study as well as an emerging field of science. Although government interest and funding in biometrics extends back over 40 years, perhaps the more recent international events evidence a need for a more sustained, predictable government interest and funding in the future.
3. Biometrics is developing into a significant industry with a very broad base of applications in a) defense and security, and b) in business process and e-commerce. Because of the pervasive nature of this technology, it is important to aggressively foster the industry with sponsored basic research.
4. Currently each biometric technology (face, voice, iris, fingerprint, etc.) uses its own jargon and methodology to the point of stifling collaboration across technologies. There is a genuine interest in standardizing the vocabulary and methodology, where possible, and such an effort would help enhance collaboration between focused research communities.

5. Standardization of terminology could bridge the synonyms used by biometric application communities and the statistical and machine learning communities. The use of "separate languages" is a hindrance to furthering the statistical enhancements necessary to advance test and evaluation of biometric systems.

Recommendations

The first recommendation is that the United States should embark on a biometric research program, addressing the items in the proposed research agenda. There are administrative issues associated with the implementation and execution of such a program, and the Federal government must soon address these issues if a scholarly biometric program is to be genuine and useful.

Biometrics should be viewed as a national resource industry. The majority of the biometric development and research in the world is going on in the US today and the government needs to take steps to ensure that this leadership is maintained for the benefit of national defense and the economy.

Biometric research is conducted according to traditional disciplines and has yet to be recognized as its own field of science. Biometrics is highly interdisciplinary, and should be viewed as a convergence of disciplines addressing interrelated issues of technology, measures of effectiveness, societal and political implications, and economics and workforce. This is a critical recommendation, and involves the creation of funded research and development programs.

This Workshop has completed its assignment notwithstanding the obvious need for development of a federal research program. It is recommended that a research program provide for the continued interaction between biometrics researchers with the perspective of biometrics as an interdisciplinary science.

TABLE 1 – List of Participants

(in addition to the Organizing Committee)

Technologies Group		
Craig	**Arndt**	Mitretek Systems
Rama	**Chelleppa**	University of Maryland
Jeff	**Dunn**	National Security Agency
Paul	**Griffin**	Identix Corp.
Larry	**Hornak**	West Virginia University
Takeo	**Kanade**	Carnegie Mellon University
Alan	**Lipton**	Object Video
Steve	**Meagher**	Federal Bureau of Investigation
Robert	**Mericsko**	Intelligence Technology Innovation Center
Lynette	**Millett**	National Academy of Sciences
Larry	**O'Gorman**	Avaya Labs
Alice	**O'Toole**	The University of Texas at Dallas
Nalini	**Ratha**	IBM Thomas J. Watson Research Center
Douglas	**Reynolds**	Massachusetts Institute of Technology
Sudeep	**Sarkar**	University of South Florida
Dale	**Setlak**	AuthenTec, Inc.
Elizabeth	**Shriberg**	SRI International
Colin	**Soutar**	Bioscrypt Inc.
Anuj	**Srivastava**	Florida State University
Gary	**Strong**	National Science Foundation
Thomas	**Vetter**	University Basel
Richard	**Wildes**	York University
Lawrence	**Wolff**	Equinox Corporation
Measures of Effectiveness Group		
Duane	**Blackburn**	Counterdrug Technology Development Program Office
Joe	**Campbell**	Massachusetts Institute of Technology
George	**Doddington**	National Institute of Standards and Technology
Stephen	**Elliott**	Purdue University
Patrick	**Grother**	National Institute of Standards and Technology
Austin	**Hicklin**	Mitretek Systems
Micheal	**Hogan**	National Institute of Standards and Technology
Tom	**Hopper**	Federal Bureau of Investigation
Satish	**Iyengar**	University of Pittsburgh
James R.	**Maar**	Baesch Computer Consulting, Inc.
Richard	**Mammone**	Rutgers University
Tony	**Mansfield**	National Physical Laboratory
Micheal	**McCabe**	National Institute of Standards and Technology
Ross	**Micheals**	National Institute of Standards and Technology
Fernando	**Podio**	National Institute of Standards and Technology
Yehuda	**Vardi**	Rutgers University
Charles	**Wilson**	National Institute of Standards and Technology
Societal and Political Implications, Economics and Workforce Group		
Richard	**Carter**	AAMVA
M. Paul	**Collier**	The Biometric Foundation
Steven	**Goldberg**	Georgetown University Law Center
Peter	**Higgins**	Higgins & Associates, Int'l
Rick	**Lazarick**	Transportation Security Administration
Martin	**Libicki**	RAND
John	**McKeon**	IBM
W. Russell	**Neuman**	White House Office of Science & Technology Policy
Donald	**Prosnitz**	Lawrence Livermore Lab
Kathleen	**Wallman**	Georgetown University Law Center

TABLE 2 – Workshop Agenda

Workshop for a Biometric Research Agenda

(April 30 – May 2, 2003 in Morgantown, WV)

Evening Registration and Reception (April 29, Tuesday)

Day 1 (April 30, Wednesday)

7:30 Registration and Breakfast

9:00 Welcome
Anil Jain and Edwin Rood, Co-Chairmen
Opening Remarks
David C. Hardesty, Jr, President, West Virginia University

9:40 Plenary Lecture: Technology Rama Chellappa, University of Maryland
"Recognition of Humans and Their Activities Using Video"

10:40 Refreshment Break

11:00 Plenary Lecture: Measures of Effectiveness (Jim Wayman)
Charles L. Wilson, National Institute of Standards and Technology
"NIST PATRIOT Act Biometric Projects"

12:00 Lunch

1:30 Plenary Lecture: Personal Liberties, Social and Economic Implications
Steve Goldberg, Georgetown University Law Center
"The Social Context of Biometrics: How the Intersection of Law and Science Shapes the Future"

2:30 Charge to the Breakout Groups (Gary Strong, NSF)
2:45 Breakout Groups meet individually to determine their agendas
(4:15 Refreshment Break)
6:00 Break

7:00 Banquet
W. Russell Neuman, Office of Science and Technology Policy, The White House
"A Tale of Three Towers"

Day 2 (May 1, Thursday)

7:30 Buffet breakfast

8:30 Breakout Groups report to the Whole as to what they are considering
9:30 Breakout Groups meet individually; prepare reports
(10:00 Refreshment Break)

12:00 Lunch
Rich Carter, Director, Technology Standards and Programs
American Association of Motor Vehicle Administrators
"Are You Also Somebody Else?"

1:30 Breakout Groups continue meeting
3:30 Refreshment Break
4:00 Reports to the Whole from Breakout Groups (Part 1)

5:30 Break, and Bus Tour of West Virginia University campuses

7:00 Banquet
Gary Strong, National Science Foundation
"Homeland Security/National Security Research at the National Science Foundation"

Day 3 (May 2, Friday)

7:30 Buffet breakfast

8:30 Reports to the Whole from Breakout Groups (Part 2)

10:00 Refreshment Break

10:20 Charge to the Writing Committee (Edwin Rood, West Virginia University)
11:00 Adjournment

11:30 Lunch