

Free Summary



Biometric Recognition: Challenges and Opportunities

Joseph N. Pato and Lynette I. Millett, Editors; Whither Biometrics Committee; National Research Council

ISBN: 978-0-309-14207-6, 182 pages, 6 x 9, paperback (2010)

This free summary is provided by the National Academies as part of our mission to educate the world on issues of science, engineering, and health. If you are interested in reading the full book, please visit us online at <http://www.nap.edu/catalog/12720.html>. You may browse and search the full, authoritative version for free; you may also purchase a print or electronic version of the book. If you have questions or just want more information about the books published by the National Academies Press, please contact our customer service department toll-free at 888-624-8373.

This summary plus thousands more available at www.nap.edu.

Copyright © National Academy of Sciences. All rights reserved. Unless otherwise indicated, all materials in this PDF file are copyrighted by the National Academy of Sciences. Distribution or copying is strictly prohibited without permission of the National Academies Press <http://www.nap.edu/permissions/>. Permission is granted for this material to be posted on a secure password-protected Web site. The content may not be posted on a public Web site.

Summary

Biometrics is the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways. Figure S.1 illustrates the basic operations of a recognition process.

Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders. The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security. Questions persist, however, about the effectiveness of biometric systems as security or surveillance mechanisms, their usability and manageability, appropriateness in widely varying contexts, social impacts, effects on privacy, and legal and policy implications.

The following are the principal conclusions of this study:

- Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated. System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent.
- The scientific basis of biometrics—from understanding the distributions of biometric traits within given populations to how humans

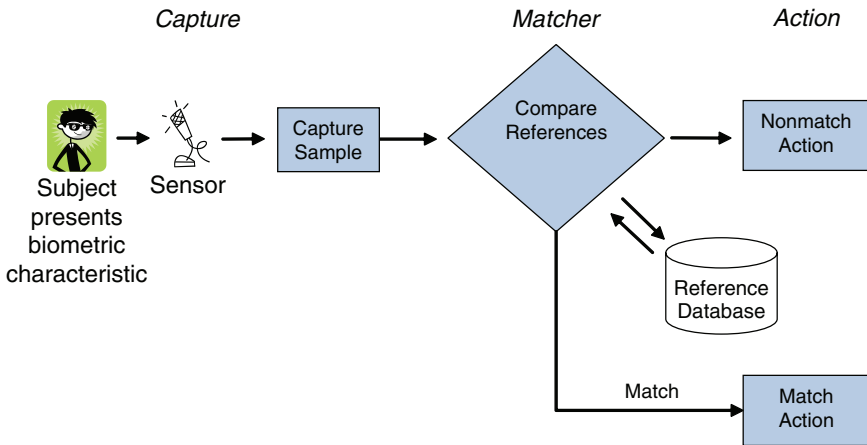


FIGURE S.1 Sample operation of a general biometric system. The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). This figure depicts the operation of a generic biometric system although some systems will differ in their particulars. The primary components for the purposes of this discussion are “capture,” where the sensor collects biometric data from the subject to be recognized; the “reference database,” where previously enrolled subjects’ biometric data are held; the “matcher,” which compares presented data to reference data in order to make a recognition decision; and “action,” where the system recognition decision is revealed and actions are undertaken based on that decision.

interact with biometric systems—needs strengthening particularly as biometric technologies and systems are deployed in systems of national importance.

- Biometric systems incorporate complex definitional, technological, and operational choices, which are themselves embedded in larger technological and social contexts. Thus, systems-level considerations are critical to the success of biometric systems. Analyses of biometric systems’ performance, effectiveness, trustworthiness, and suitability should take a broad systems perspective.

- Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes.

- The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation. Presumptions and burdens of proof arising from biometric

recognition should be based on solid, peer-reviewed studies of the performance of biometric recognition mechanisms.

FUNDAMENTALS OF BIOMETRIC RECOGNITION AND HUMAN INDIVIDUAL DISTINCTIVENESS

Biometric recognition systems are inherently probabilistic, and their performance needs to be assessed within the context of this fundamental and critical characteristic. Biometric recognition involves matching, within a tolerance of approximation, of observed biometric traits against previously collected data for a subject. Approximate matching is required due to the variations in biological attributes and behaviors both within and between persons.¹ Consequently, in contrast to the largely binary results associated with most information technology systems, biometric systems provide probabilistic results.

There are numerous sources of uncertainty and variation in biometric systems, including the following:

- *Variation within persons.* Biometric characteristics and the information captured by biometric systems may be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, sociocultural aspects of the situation in which the presentation occurs, changes in human interface with the system, and so on. As a result, each interaction of the individual with the system (at enrollment, identification, and so on) will be associated with different biometric information. Individuals attempting to thwart recognition for one reason or another also contribute to the inherent uncertainty in biometric systems.

- *Sensors.* Sensor age and calibration, how well the interface at any given time mitigates extraneous factors, and the sensitivity of sensor performance to variation in the ambient environment (such as light levels) all can play a role.

- *Feature extraction and matching algorithms.* Biometric characteristics cannot be directly compared but require stable and distinctive “features” to first be extracted from sensor outputs. Differences in feature extraction algorithms affect performance, with effects sometimes aggravated by requirements for achieving interoperability among proprietary systems. Differences between matching algorithms and comparison scoring mecha-

¹For example, each finger of each person will generate a different fingerprint image every time it is observed due to presentation angle, pressure, dirt, moisture, different sensors, and so on. Thus each person can produce a large number of different impressions from a single finger—many of which will be close enough that good algorithms can match them to the correct finger source.

nisms, and how these interact with the preceding sources of variability of information acquired and features extracted, also contribute to variation in performance of different systems.

- *Data integrity.* Information may be degraded through legitimate data manipulation or transformation or degraded and/or corrupted owing to security breaches, mismanagement, inappropriate compression, or some other means. It may also be inappropriately applied to a context other than the one for which it was originally created, owing to mission creep (for example, using the data collected in a domain purely for the sake of convenience in a domain that demands high data integrity) or inappropriate re-use of information (for instance, captured biometric information might be incorrectly assumed to be of greater fidelity when transferred to a system where higher fidelity is the norm).

Many gaps exist in our understanding of the nature and extent of distinctiveness and stability of biometric traits across individuals and groups. No biometric characteristic is known to be entirely stable and distinctive across all groups. Biometric traits have fundamental statistical properties, distinctiveness, and differing degrees of stability under natural physiological conditions and environmental challenges, many aspects of which are not well understood, especially at large scales. Complicating matters, the underlying biological properties and distribution of biometric traits in a population are generally observed only through filters interposed by measurement processes and instruments and subsequent biometric feature extraction.

Thus, the development of a science of human individual distinctiveness is essential to effective and appropriate use of biometric recognition. Better understanding of biometric traits in human beings could be gained by carefully designed data collection and analysis. The biological underpinnings of physical distinctiveness and the stability of many biometric characteristics under natural physiological conditions and environmental challenges require further justification from basic biological and empirical studies. Importantly, the underlying distinctiveness of a biometric trait cannot be assessed apart from an understanding of the stability, accuracy, and inherent variability of a given measure.

Another fundamental characteristic of biometric recognition is that it requires decision making under uncertainty by both the automated recognition system and the human interpreters of its results. A biometric match represents not certain recognition but a probability of correct recognition, while a nonmatch represents a probability rather than a definitive conclusion that an individual is not known to the system. That is, some fraction of results from even the best-designed biometric system will be incorrect or indeterminate: both false matches and false nonmatches will occur. Moreover, assessing the validity of the match results, even given

this inherent uncertainty, requires knowledge of the population of users who are presenting to the system—specifically, what proportions of those users should and should not match. Even very small probabilities of misrecognitions—the failure to recognize an enrolled individual or the recognition of one individual as another—can become operationally significant when an application is scaled to handle millions of recognition attempts. Thus, well-articulated processes for verification, mitigation of undesired outcomes, and remediation (for misrecognitions) are needed, and presumptions and burdens of proof should be designed conservatively, with due attention to the system’s inevitable uncertainties.

Principle: Users and developers of biometric systems should recognize and take into account the limitations and constraints of biometric systems—especially the probabilistic nature of the underlying science, the current limits of knowledge regarding human individual distinctiveness, and the numerous sources of uncertainty in biometric systems.

BIOMETRIC SYSTEMS AND TRUSTWORTHINESS

Systems that perform biometric recognition exist within a constellation of other authentication and identification technologies and offer some distinct capabilities and challenges. Authentication technologies are typically based on one of three things: something the individual knows, such as a password; something the individual has, such as a physical key or secure token; and something the individual is or does.² Biometric technologies employ the last of these. Unlike password- or token-based systems, biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place.

Biometric systems, therefore, are not a general replacement for other authentication technologies, although combining biometric approaches with other methods can augment security in those applications where user cooperation can be inferred.

One important difference between biometric and other authentication technologies, such as tokens or passwords, is that these other technologies place trust in cooperative users, allowing them to produce what they possess or demonstrate what they know (through dependence on the user’s safekeeping of a card or password). But these other forms of authentication do not protect against the sharing or transfer of the token or secret,

²Federal Information Processing Standards 48, “Guidelines on Evaluation of Techniques for Automated Personal Identification,” was published in 1977 and was one of the first such treatments of authentication.

whereas biometric traits are tied to an individual³—specifically something an individual is or does.⁴ Unintended disclosure of biometric data, however, may lead to more serious consequences or to consequences that are more difficult to remediate than the loss of a token or exposure of a password. Another important difference is that because they are probabilistic, biometric systems are particularly vulnerable to deliberate attempts to undermine confidence in their reliability, and discussions of probabilistic uncertainty can easily be twisted into a suggestion that biometric systems are unreliable.

Security challenges for biometric systems can be seen as stemming from two different views of such systems: (1) the use of biometric systems as a security mechanism to protect information systems or other resources and (2) vulnerabilities of the biometric system itself. First, it is necessary to determine if a biometric system is an appropriate component for the application at hand at all. One needs to specify the problem to be solved by a particular biometric system in order to adequately assess its effectiveness and deal with the consequences of deployment.⁵ Conducting a threat analysis and developing threat models for the system that incorporates analysis of feasibility of threats against the resource being protected and against the system doing the protecting is an important component of understanding the problem. Decisions about whether and how to incorporate biometric approaches should consider their appropriateness and proportionality given the problem to be solved and the merits and risks of biometrics relative to other solutions⁶ and need to be considered by the broader information security community as well as within the biometrics community.

Second, biometric systems (and not merely the resources they are protecting) are themselves vulnerable to attacks aimed at undermining their integrity and reliability. For password- or token-based systems, a breach can usually be remediated by issuing a new password or token.

³While it is possible to copy or mimic some biometric traits, it is generally more difficult to produce such a trait and present it to a supervised sensor than to share a password or token. If the system is unsupervised, an attacker may not need to spoof the trait physically; he might have a copy of the bit string or the reference, which would make such an attack no more difficult than compromising other forms of recognition.

⁴More precisely, biometric authentication is a binary hypothesis test where the hypothesis is that the biometric sample input matches—to a degree of certainty—the claimed biometric reference enrollment. The overall system then uses the matching results to accept or reject this hypothesis.

⁵See *Who Goes There? Authentication Through the Lens of Privacy and IDs—Not That Easy* for discussions of the need to understand the problem that a system is trying to solve in order to evaluate the system's effectiveness.

⁶For example, the problem of managing members' access to a local health club merits different kinds of analysis than does handling customs and immigration at a major international airport.

However, it is generally not possible to replace a biometric trait that has been compromised. This is complicated by the fact that the same biometric trait can be used by different systems, and weaknesses in one system could lead to the compromise of the biometric trait for use in another system. Furthermore, such traits are not secret—we expose them in the course of everyday life. For example, we leave fingerprints on many surfaces we touch, faces can be photographed, and voices can be recorded. However, it is as difficult for an impostor to grow a set of fingerprints matching those stolen as it is for the person they were stolen from to grow a new and different set. It is, accordingly, essential to validate that a trait presented to gain recognition truly belongs to the subject and is not being synthesized by an impostor. This often requires a human operator to observe the subject's presentation of the trait—which significantly constrains remote or distributed applications of biometrics. Automated verification that a living person is presenting what could conceivably be a synthesized artifact might be sufficient in some applications but would not substitute for human supervision where high degrees of confidence are required.

It is important to manage the trustworthiness of the entire process rather than focusing on evaluation of the proffered biometric characteristic. Systems using biometric recognition are typically designed with alternative procedures for use when a sensor fails or an individual lacks the biometric trait. Adversaries may attempt to force the system into failure modes to evade or accomplish recognition, implying that secondary screening procedures should be just as robustly designed as the main procedure. One potential way to improve recognition would be to use multiple biometric modalities and other demographic data to narrow the search space. This approach might have other advantages, such as expanding population coverage beyond that afforded by a single biometric and reducing vulnerability to spoofing attacks. It might have disadvantages, as well, including increasing the complexity and cost of the system. There are also issues related to the architecture and operation of multibiometrics systems as well as questions of how best to model such systems and then use the model to drive operational aspects. Understanding any statistical dependencies is critical when using multibiometrics.

TESTING, DESIGN, AND DEPLOYMENT

Although traditional biometrics testing tends to focus on the match performance for a test data set, experience from many domains suggests that process and quality control should be analyzed for the complete system life cycle. Methods used successfully for the study and improvement of systems in other fields such as manufacturing and medicine (for example, controlled observation and experimentation on operational

systems guided by scientific principles and statistical design and monitoring) should be used in developing, maintaining, assessing, and improving biometric systems. One especially important lesson is that testing methods and results should be sufficiently open to allow independent assessment.

Although laboratory evaluations of biometric systems are highly useful for development and comparison, their results often do not reliably predict field performance. Operational testing and blind challenges of operational systems tend to give more accurate and usable results than developmental performance evaluations and operational testing in circumscribed and controlled environments. Although the international standards community has made progress in developing a coherent set of best practices for technology and scenario testing, guidelines for operational testing are still under development.⁷ Designing a system and tests that can cope with ongoing data collection, particularly at scale, is a challenge making it difficult for a potential user of biometrics to determine how well a vendor's technology might operate in that user's applications or to measure improvements in the system's performance.

Principle: Efforts to determine best practices for testing and evaluating existing and new biometric systems should be sustained and expanded. Careful consideration should be given to making the testing process open, allowing assessment of results and quality measures by outside parties when appropriate. The evaluation of a system's effectiveness needs to take into account the purpose for which the system was developed and how well field conditions were matched.

It is essential to take a broad systems view when assessing the performance of biometric systems. Both enthusiasm for biometric recognition and concerns about it tend to focus narrowly on behavioral and biological characteristics, human interactions with biometric sensors, or how information collected will be used. Yet the effective use of biometrics involves more than simply engineering a system to provide these basic capabilities. Achieving automated recognition involves the proper functioning of a broader system with many elements, including the human sources of data, human operators of the system, the collection environment(s), biometric sensors, the quality of the system's various technological components, the human-sensor-environment interaction, biometric reference information databases and the quality and integrity of the data therein, the system's security and availability, the system's communications network(s), and the system's failure-handling and error-recovery processes.

⁷As of this writing, ISO/IEC Standard 19794-5 for operational testing is under development by ISO/IEC JTC1 SC37.

Successful deployments have good project management and definition of goals, alignment of biometric capabilities with the underlying need and operational environment, and a thorough threat and risk analysis. Failure is often rooted in a lack of clarity about the problem being addressed, lack of a viable business case, inappropriate application of biometrics where other technologies would work better, inappropriate choice of biometric technologies, insensitivity to user perceptions and usability requirements, inadequate support processes and infrastructure, and/or poor understanding of population issues among those to be recognized. User behavior, attitudes, and system usability contribute to misrecognitions, and how incorrect or indeterminate results are handled contributes to whether a system's goals are met.

The probabilistic nature of biometric systems makes them especially sensitive to how well exception mechanisms are implemented. In particular, the inevitable false matches, false nonmatches, and failures to enroll are likely to stress other portions of the system that have been put in place to compensate when such errors occur. Field error rates are likely to be higher than laboratory testing suggests, poor exception processes can negate benefits, and extrapolation of functions in one context to another context may be inappropriate.

Biometric systems should be designed to anticipate the development and adoption of new advances and standards, modularizing components that are likely to become obsolete, such as biometric sensors and matcher systems, so that they can be easily replaced. A life-cycle approach such as this requires understanding and taking into account the capabilities and limitations of biometric technologies and devices. Some of the factors that may compromise later use if systems are not backwards-compatible include degradation of data through transformations due to system interconnection or changes in technology and reuse of data in unanticipated applications. Exception policies, data quality threshold settings, and the consequences of false matches and false nonmatches may need adjustment over the life of a deployment, and provisions for such adjustments should be included in the system design. Training and outreach materials for a nonscientific audience are needed, along with strategies for dissemination to system operators. A life-cycle-oriented approach should also be flexible enough to manage the unexpected reactions of users, operators, or other stakeholders.

Principle: Best practices are needed for the design and development of biometric systems and the processes for their operation. To scale efficiently to mass applications, these best practices should include requirements for system usability, initial and sustained technical accuracy and system performance, appropriate exception handling, and consistency of adjudication at the system level. Best practices should allow for incorpo-

ration of scientific advances and be auditable throughout the life of the system.

System requirements can range widely depending on the user context, the application context, and the technology context. Issues related to the user context include motivations for using the system, users' awareness of their interactions with a system, and training and habituation to its use. Issues related to the application context include whether the system is supervised by human staff, whether it is being used to verify a positive recognition claim or a negative one, whether the population to be recognized is an open or closed group, and whether testing the claim requires one comparison or many. Issues related to the technology context include whether the environment (say, the lighting) is controlled, whether the system is covert or overt, passive or active (requiring interaction with the subject), how quickly users need to be processed, and the error rates required (based, for instance, on the consequence of errors). The issues related to these contexts should affect the system design, development, and deployment. In particular, the wide variety of options for a biometric system encompassed above make clear that the incorporation of biometrics in a system in and of itself says very little about the requirements or usage expectations of that system.

Principle: Requirements have critical implications for the design and development of human recognition systems and whether and how biometric technologies are appropriately employed. Requirements for systems can vary widely, and assessment and evaluation of the effectiveness of a given system need to take into account the problem and context it was intended to address.

SOCIAL, CULTURAL, AND LEGAL CONSIDERATIONS

Although biometric systems can be beneficial, the potentially lifelong association of biometric traits with an individual, their potential use for remote detection, and their connection with identity records may raise social, cultural, and legal concerns. When used in contexts where individuals are claiming enrollment or entitlement to a benefit, biometric systems could disenfranchise people who are unable to participate for physical, social, or cultural reasons. For these reasons, the use of biometrics—especially in applications driven by public policy, where the affected population may have little alternative to participation—merits careful oversight and public discussion to anticipate and minimize detrimental societal and individual effects and to avoid violating privacy and due process rights.

Social, cultural, and legal issues can affect a system's acceptance by

users, its performance, or the decisions on whether to use it in the first place—so it is best to consider these explicitly in system design. Clearly, the behavior of those being enrolled and recognized can influence the accuracy and effectiveness of virtually any biometric system, and user behavior can be affected by the social, cultural, or legal context. Likewise, the acceptability of a biometric system depends on the social and cultural values of the participant populations. A careful analysis and articulation of these issues and their trade-offs can improve both acceptability and effectiveness. Moreover, the benefits arising from using a biometric system may flow to particular individuals or groups, sometimes only at the expense of others—for example, a building’s owner might be more secure but at the cost of time and inconvenience to those who wish to enter the building—making calculating these trade-offs more difficult.

Fundamental to most social issues surrounding biometric recognition is the tight link between an individual’s biometric traits and data record, which can have positive and negative consequences. These consequences can affect the disposition of a target population toward a particular application. The potential for disenfranchisement means that some could be excluded from the benefits of positive claim systems, including access to buildings and information or qualification for jobs or insurance. Policies and interfaces to handle error conditions such as failure to enroll or be recognized should be designed to gracefully avoid violating the dignity, privacy, or due process rights of the participants. In addition, the potential for abuse of power is a cause for concern. Many fear misuse of identification technology by authorities (from data compromise, mission creep, or use of a biometric for other than specified purposes). To be effective, biometric deployments need to take these fears seriously.

Some biometric systems are designed to recognize and track individuals without their knowledge. Covert identification has not been widely deployed, but its potential raises deep concerns. Although the biometrics industry has at times dismissed such concerns, biometric systems could win broader acceptance if more attention were paid to the target community’s cultural values.

Biometric recognition raises important legal issues of remediation, authority, and reliability, and, of course, privacy. The standard assumptions of the technologists who design new techniques, capabilities, and systems are very different from those embedded in the legal system. Legal precedent on the use of biometric technology is growing, with some key cases going back decades,⁸ and other more recent cases⁹ having raised serious questions about the admissibility of biometric evidence in court.

⁸Cases include *U.S. v. Dionisio* (U.S. Supreme Court, 1973) and *Perkey v. Department of Motor Vehicles* (California Supreme Court, 1986).

⁹Such as *Maryland v. Rose* (Maryland Circuit Court, 2007).

Remediation is one way of dealing with fraudulent use of biometrics (such as identity fraud or altering biometric reference data). Remediation also deals with individuals denied their due rights or access because of an incorrect match or nonmatch. Policy and law should not only address the perpetrators of fraud but also induce system owners to minimize misuse of biometric samples and to maximize appropriate monitoring of biometric sample presentation at enrollment and participation.

The reliability of biometric recognition is clouded by the presumption of near-infallibility promoted by popular culture. Such presumptions could make contesting improper identifications excessively difficult. Conversely, if all evidence must be up to the standards implied by certain popular culture phenomena, unreasonable difficulties could be faced in cases lacking sufficient resources or evidence to meet those standards.

The courts have sometimes taken the view that an individual's expectation of privacy is related to the ubiquity of a technical means, which implies that the legal status of challenges to biometric technologies could be affected by the commonality of their use.

Principle: Social, legal, and cultural factors can affect the acceptance and effectiveness of biometric systems and should be taken into account in system design, development, and deployment. Notions of proof related to biometric recognition should be based on solid, peer-reviewed studies of system accuracy under many conditions and for many persons reflecting real-world sources of error and uncertainty in those mechanisms. Pending scientific consensus on the reliability of biometric recognition mechanisms, a reasonable level of uncertainty should be acknowledged for biometric recognition. There may be a need for legislation to protect against the theft or fraudulent use of biometric systems and data.

ELEMENTS OF A NATIONAL RESEARCH AND PUBLIC POLICY AGENDA

Given the concerns about homeland security, confidentiality of proprietary information, and fraud in general, biometric recognition is becoming a routine method of recognizing individuals. If there is a pressing public policy need for which biometric systems are the most appropriate solution, understanding the science and technology issues is critical. As the preceding discussions should make clear, many questions remain.

The committee believes that more research into performance and robustness is needed. The lack of well-defined operational best practices based on solid science may allow governments and private organizations to issue overly vague or unrealistic mandates for biometric programs leading to poorly targeted oversight, delayed and troubled programs,

excessive costs due to under- or overspecification of requirements, and failed deployments.

In short, the scientific basis of biometrics should be strengthened. Basic research should be done on the stability and distinctiveness of biometric traits; the control of environmental noise when acquiring samples; the correlation of biometric traits with private information, including medical conditions; and the demographic variability of biometric traits. Many fields of inquiry are relevant, even integral, to deepening the science of biometric recognition, including sensor design, signal processing, pattern recognition, human factors, statistics and biostatistics, computer systems design, information security, operations research, economics, politics, applied psychology, sociology, education, and the law.

Biometric systems perform well in many existing applications, but biometric capabilities and limitations are not yet well understood in very large scale applications involving tens of millions of users. Questions remain about whether today's biometric systems are sufficiently robust, able to handle errors when the consequences are severe. Although fingerprinting technology has been applied on a large scale for decades in law enforcement, human experts are available in this application to help process noisy or difficult samples. Even so, there have been a few high-profile misidentifications with serious ramifications. It remains to be seen if fully automatic biometric systems can meet performance requirements as the number and scale of deployments increase.

As mentioned above, a scientific basis for the distinctiveness and stability of various biometric traits under a variety of collection processes and environments and across a wide population over decades is needed. How accurately can a biometric trait be measured in a realistic operating environment? The individuality of biometric traits, their long- and short-term physiological and pathological variability, their relationship to the providing population's genetic makeup, health, and other private attributes all merit research attention, which will require extensive data collection. The privacy protections to be afforded participants in such data collection need to be clearly outlined.

Improvements to biometric sensors and to the quality of the data acquired are crucial to minimizing recognition errors. Sensors should be made usable by a wider range of individuals in more environments and should be able to capture more faithfully (that is, with higher resolutions and with lower noise) underlying biometric traits of more than one kind in adverse situations and at a distance. Because many applications involve large numbers of sensors, attention should be paid to the development of low-cost but high-quality sensors. Additional areas meriting attention include representation and storage improvements and match-algorithm improvements.

Understanding how users interact with systems also merits further attention. The characteristics of the subject population, their attitudes and level of cooperation, the deployment environment, and procedures for measuring performance can all affect the system. Consequently, observation and experimentation in operational systems are required to understand how well biometric applications satisfy their requirements. Because of the challenges inherent in closely observing individuals, with or without their cooperation, human factors are critical to the design of processes for monitoring subjects and operators when assessing the effectiveness of a biometric system.

Another area where research is required is in the systems' view of biometric recognition, encompassing social, legal, and cultural aspects. Related are social implications of biometric recognition on a large scale. Research is needed, too, on the distinctive information security problems of biometric systems, such as defense against attacks by individuals using fake or previously captured biometric samples and the concealment of biometric traits, and on the protection of biometric reference databases. Decision analysis and threat modeling are other critical areas requiring research advances.

The U.S. government has created or funded several interdisciplinary, academically based research programs that provide a foundation for future work. Research support should aim for greater involvement of scientists and practitioners from relevant disciplines in biometric research, and studies should be published in the open, peer-reviewed scientific literature, with their stringently deidentified biometric samples made widely available to other researchers. A clearinghouse would facilitate efforts toward identifying standards implementation and interoperability issues, characterizing common elements of successful implementations, cataloging lessons learned, and maintaining data as input for testing product robustness and system performance.

Principle: As biometric recognition is deployed in systems of national importance, additional research is needed at virtually all levels of the system (including sensors, data management, human factors, and testing). The research should look at a range of questions from the distinctiveness of biometric traits to optimal ways of evaluating and maintaining large systems over many years.

Biometric Recognition

CHALLENGES AND OPPORTUNITIES

EMBARGOED—NOT FOR PUBLIC RELEASE
UNTIL 11 AM EDT FRIDAY, SEPTEMBER 24, 2010

Joseph N. Pato and Lynette I. Millett, *Editors*

Whither Biometrics Committee

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the Defense Advanced Research Projects Agency (Award No. N00174-03-C-0074) and by the Central Intelligence Agency and the Department of Homeland Security with assistance from the National Science Foundation (Award No. IIS-0344584). Any opinions expressed in this material are those of the authors and do not necessarily reflect the views of the agencies and organizations that provided support for the project.

International Standard Book Number-13: 978-0-309-14207-6

International Standard Book Number-10: 0-309-14207-5

Copies of this report are available from

The National Academies Press
500 Fifth Street, N.W., Lockbox 285
Washington, DC 20055
800/624-6242
202/334-3313 (in the Washington metropolitan area)
<http://www.nap.edu>

Copyright 2010 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

WHITHER BIOMETRICS COMMITTEE

JOSEPH N. PATO, Hewlett-Packard Company, *Chair*
BOB BLAKLEY, Gartner
JEANETTE BLOMBERG, IBM Almaden Research Center
JOSEPH P. CAMPBELL, Massachusetts Institute of Technology, Lincoln
Laboratory
GEORGE T. DUNCAN, Carnegie Mellon University
GEORGE R. FISHER, Prudential-Wachovia (retired)
STEVEN P. GOLDBERG,¹ Georgetown University Law Center
PETER T. HIGGINS, Higgins & Associates, International
PETER B. IMREY, Cleveland Clinic and Case Western Reserve
University
ANIL K. JAIN, Michigan State University
GORDON LEVIN, The Walt Disney World Company
LAWRENCE D. NADEL, Noblis
JAMES L. WAYMAN, San Jose State University

Staff

LYNETTE I. MILLETT, Senior Program Officer

¹ Steven P. Goldberg died on August 26, 2010.

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

ROBERT F. SPROULL, Oracle Corporation, *Chair*
PRITHVIRAJ BANERJEE, Hewlett-Packard Company
STEVEN M. BELLOVIN, Columbia University
SEYMOUR E. GOODMAN, Georgia Institute of Technology
JOHN E. KELLY III, IBM
JON M. KLEINBERG, Cornell University
ROBERT KRAUT, Carnegie Mellon University
SUSAN LANDAU, Radcliffe Institute for Advanced Study
DAVID E. LIDDLE, US Venture Partners
WILLIAM H. PRESS, University of Texas, Austin
PRABHAKAR RAGHAVAN, Yahoo! Labs
DAVID E. SHAW, D.E. Shaw Research
ALFRED Z. SPECTOR, Google, Inc.
JOHN A. SWAINSON, Silver Lake
PETER SZOLOVITS, Massachusetts Institute of Technology
PETER J. WEINBERGER, Google, Inc.
ERNEST J. WILSON, University of Southern California

Staff

JON EISENBERG, Director
VIRGINIA BACON TALATI, Associate Program Officer
SHENAE BRADLEY, Senior Program Assistant
RENEE HAWKINS, Financial and Administrative Manager
HERBERT S. LIN, Chief Scientist
EMILY ANN MEYER, Program Officer
LYNETTE I. MILLETT, Senior Program Officer
ERIC WHITAKER, Senior Program Assistant
ENITA A. WILLIAMS, Associate Program Officer

For more information on CSTB, see its website at
<http://www.cstb.org>, write to CSTB, National Research
Council, 500 Fifth Street, N.W., Washington, DC 20001, call
(202) 334-2605, or e-mail the CSTB at cstb@nas.edu.

Preface

In a variety of government and private domains biometric recognition is being promoted as a technology that can help identify terrorists, provide better control of access to physical facilities and financial accounts, and increase the efficiency of access to services and their utilization. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things. In spite of substantial effort, however, there remain unresolved questions about the effectiveness and management of systems for biometric recognition, as well as the appropriateness and societal impact of their use. Moreover, the general public has been exposed to biometrics largely as high-technology gadgets in spy thrillers or as fear-instilling instruments of state or corporate surveillance in speculative fiction.

Now, at the beginning of the second decade of the twenty-first century, biometric technologies appear poised for broader use. Increased concerns about national security and the tracking of individuals as they cross borders have caused passports, visas, and border-crossing records to be linked to biometric data. A focus on fighting insurgencies and terrorism has led to the military deployment of biometric tools to enable recognition of individuals as friend or foe. Commercially, finger-imaging sensors, whose cost and physical size have been reduced, now appear on many laptop personal computers, handheld devices, mobile phones, and other consumer devices.

In 2001 the Computer Science and Telecommunications Board (CSTB)

of the National Research Council (NRC) formed a committee whose 2003 report *Who Goes There? Authentication Through the Lens of Privacy*, considered several authentication technologies, one of which was biometrics. After the publication of that report, the CSTB held several discussions with various federal agencies interested in biometrics. Jonathon Phillips (then at the Defense Advanced Research Projects Agency (DARPA)), Gary Strong (then at the Department of Homeland Security (DHS)), and Andrew Kirby (of the Central Intelligence Agency (CIA)) actively participated in the discussions and helped to move them forward. The discussions resulted in agreement to undertake this comprehensive assessment of biometrics (see Appendix C for the project's original statement of task). Funding for the project was obtained from DARPA and from the CIA and the DHS with assistance from the National Science Foundation. The Whither Biometrics Committee was formed to conduct the study.

The Whither Biometrics Committee consisted of 13 members¹ from industry and academia who are experts in different aspects of distributed systems, computer security, biometrics (of various flavors), systems engineering, human factors, the law, and statistics, as well as in computer science and engineering (see Appendix A for committee and staff biographies).

Early in the study the committee organized a public workshop. Held on March 15 and 16, 2005, in Washington, D.C., the workshop was attended by members of industry, government, and academia and reported on by the committee in *Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric Systems*.² In the course of the study, inputs were gathered on the challenges, capabilities, and requirements of biometric systems as well as related policy and social questions. This report draws on what was learned at the workshop and in subsequent briefings to the committee.

The report makes two main points. First, developers and analysts of biometric recognition systems must bear in mind that such systems are complex and need to be addressed as such. Second, biometric recognition is an inherently probabilistic endeavor. The automated recognition of individuals offered by biometric systems must be tempered by an awareness of the uncertainty associated with that recognition. Uncertainty arises in numerous ways in biometric systems, including from poor or incomplete understanding of the distinctiveness and stability of the traits measured

¹Delores Etter was originally a member of the committee but resigned when she was appointed Assistant Secretary of Research, Development, and Acquisition for the U.S. Navy.

²National Research Council, *Summary of a Workshop on the Technology, Policy, and Cultural Dimensions of Biometric Systems*, Kristen Batch, Lynette I. Millett, and Joseph N. Pato, eds., The National Academies Press, Washington, D.C., 2006.

by biometric systems; the difficulty of characterizing the probability that an imposter will attack the system; and even the attitudes of the subjects using the systems—subjects who may have become conditioned by fictional depictions to expect, or even fear, that recognition will be perfect. Consequently, even when the technology and the system it is embedded in are behaving as designed, there is inevitable uncertainty and risk of error. The probabilistic nature of biometric systems also means that the measured characteristics of the population of intended users (those the system is designed to recognize) matter and affect design and implementation choices.

This report elaborates on these themes in detail and is aimed at a broad audience, including policy makers, developers, and researchers. For policy makers, it seeks to provide a comprehensive assessment of biometric recognition that examines current capabilities, future possibilities, and the role of government in technology and system development. For developers and researchers, the report's goals are to articulate challenges posed by understanding and developing biometric recognition systems and to point out opportunities for research. Building on CSTB's work on authentication technologies and privacy, it explores the technical and policy challenges associated with the development, evaluation, and use of biometric technologies and systems that incorporate them.

The committee members brought different and complementary perspectives to their efforts as they deliberated and solicited input from a number of other experts. The committee held six plenary meetings, including the workshop. It thanks the many individuals who contributed, including the project sponsors that enabled this activity. The committee also conducted three site visits, one to the Boston Police Department's Identification Center, one to the U.S. Naval Academy, and another to Walt Disney World. The committee thanks those who came and briefed the committee at those meetings and site visits: Andrew Kirby, Joseph Kielman, John Atkins, Martin Herman, Duane Blackburn, Jean-Christophe Fondeur, James Matey, Sharath Pankanti, Jonathon Phillips, David Scott, George Doddington, Michele Freadman, Patrick Grother, Austin Hicklin, Nell Sedransk, Tora Bikson, David Kaye, Lisa Nelson, Peter Swire, Joseph Atick, Rick Lazarick, Tony Mansfield, Marek Rejman-Greene, Valorie Valencia, Cynthia Musselman, William Casey, Patty Cogswell, Neal Latta, K.A. Taipale, John Woodward, Jim Dempsey, Ari Schwartz, Michael Cherry, Mike Labonge, Richard Nawrot, Diane Ley, John Schmitt, Michael Wong, Vance Bjorn, Betty LaCrois, Ken Fong, Joseph Dahlbeck, Dennis Treece, and Lynne Hare. It appreciates briefers' willingness to answer the questions they were asked and is grateful for their insights. Additional information was garnered from reviewing the published literature and obtaining informal input at various conferences and other meetings. Input

was also derived from committee members during the course of their professional activities outside the committee's work.

It is with great sadness that we mourn the passing of our colleague and fellow committee member Steven Goldberg, who died just prior to this report's publication. He was a valued member of our study team. His insights on science and the law and his collegial and constructive approach to interdisciplinary work are greatly missed.

We thank the sponsors who enabled this project, the reviewers whose constructive criticism improved the report, and the editor Liz Fikre for her help in refining the final draft of the report. The committee is grateful to the CSTB staff members whose work has made this report possible. The committee thanks Jon Eisenberg for his extensive helpful feedback throughout the process, Margaret Huynh for impeccable coordination of logistics, Kristen Batch for her work in assisting with our earlier workshop report, and Ted Schmitt, who helped structure early drafts of the final report. Finally, we thank Lynette Millett, Senior Program Officer, who has ably guided this project as study director from its inception and was essential to completing our work.

Joseph N. Pato, *Chair*
Whither Biometrics Committee

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Michael F. Angelo, Net IQ,
Ming Hsieh, Cogent Systems, Inc.,
Stephen Kent, BBN Technologies,
Sara Kiesler, Carnegie Mellon University,
Herbert Levinson, Transportation Consultant,
Steven Lipner, Microsoft Corporation,
Helen Nissenbaum, New York University,
Louise Ryan, Harvard School of Public Health,
Michael Saks, Arizona State University, and
Valorie Valencia, Authenti-Corp.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclu-

sions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Robert F. Sproull of Oracle Corporation. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

SUMMARY	1
1 INTRODUCTION AND FUNDAMENTAL CONCEPTS	15
The Systems Perspective, 19	
Motivations for Using Biometric Systems, 20	
Human Identity and Biometrics, 22	
The Fundamental Dogma of Biometrics, 23	
Basic Operational Concepts, 24	
Sample Operational Process, 25	
Measures of Operational Efficacy, 26	
Variability and Uncertainty, 27	
Within- and Between-Person Variability, 28	
Stability and Distinctiveness at Global Scale, 30	
Biometric Modalities, 31	
Comparison of Modalities, 34	
Multibiometrics, 35	
Coping with the Probabilistic Nature of Biometric Systems, 36	
Additional Implications for Open-Set Identification Systems, 45	
Security and Threat Modeling, 47	
On Report Scope and Boundaries, 52	
2 ENGINEERING BIOMETRIC SYSTEMS	53
Basic Biometric System Operations, 54	
Enrollment Operations, 54	

	Capture and Matching Operations, 58	
	Operational Context, 59	
	User Context, 60	
	Application Context, 62	
	Technology Context, 64	
	Performance Context, 65	
	Interoperability, 66	
	Sensor Interoperability, 66	
	Human Interface Interoperability, 68	
	System Life-Cycle Issues, 68	
	Test and Evaluation, 70	
	Usability Evaluations, 73	
	Test and Evaluation Standards, 73	
	Performance Assessment and Evaluation, 74	
3	LESSONS FROM OTHER LARGE-SCALE SYSTEMS	76
	Manufacturing Systems, 77	
	Medical Screening Systems, 81	
4	CULTURAL, SOCIAL, AND LEGAL CONSIDERATIONS	85
	Interaction Between Biometric Systems and Individuals, 86	
	Motivating Participation by Individuals, 86	
	Facilitating Individual Participation, 87	
	Societal Impact, 89	
	Universality and Potential Disenfranchisement, 89	
	Privacy as a Cultural Consideration, 90	
	Individuality and Identity, 93	
	Legal Issues, 95	
	Reliability, 96	
	Privacy in a Legal Context and Potential Implications for Biometrics, 100	
	Data Policies, 111	
	Information-Sharing Issues, 112	
	Protection of Biometric Data, 114	
	Summary, 115	
5	RESEARCH OPPORTUNITIES AND THE FUTURE OF BIOMETRICS	116
	Technology and Engineering Research Opportunities, 117	
	Human Factors and Affordance, 118	
	Distinctiveness and Stability of Underlying Phenomena, 119	
	Modality-Related Research, 121	
	Information Security Research, 122	

Testing and Evaluation Research, 123	
Systems-Level Statistical Engineering Research, 129	
Research on Scale, 130	
Social Science Research Opportunities, 132	
Public Policy Considerations and Research Opportunities, 135	
Realizing a Well-Designed Biometric System, 137	
Concluding Remarks, 138	

APPENDIXES

A Biosketches of Committee Members and Staff	141
B Watch-List Operational Performance and List Size	150
C Statement of Task	154
D Testing and Evaluation Examples	155
E The Biometrics Standards Landscape	159

