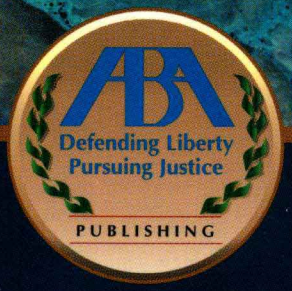
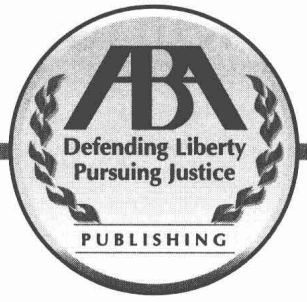


The Practitioner's Guide to Biometrics

William Sloan Coats
Amy Bagdasarian
Tarek J. Helou
and Taryn Lam

ABA Section of
Science & Technology Law



The Practitioner's Guide to Biometrics

William Sloan Coats
Amy Bagdasarian
Tarek Helou
and Taryn Lam

ABA SECTION OF
SCIENCE & TECHNOLOGY LAW

Cover design by ABA Publishing

11 10 09 08 07 5 4 3 2 1

Cataloging-in-Publication data is on file with the Library of Congress.

Biometrics / William Sloan Coats, editor

Discounts are available for books ordered in bulk. Special consideration is given to state bars, CLE programs, and other bar-related organizations. Inquire at Book Publishing, ABA Publishing, American Bar Association, 321 North Clark Street, Chicago, Illinois 60610.

www.ababooks.org

About the Editors

Amy Bagdasarian is an associate in the Palo Alto office of White & Case LLP. Her practice focuses on intellectual property litigation, including patent, trade secret, and copyright litigation. Ms. Bagdasarian has assisted in the representation of diverse high-technology clients in software, video imaging, portable electronics, semiconductor chip technology, and biomedical technology, among other industries.

Ms. Bagdasarian received her bachelor of arts degree from UCLA and her juris doctor degree from Santa Clara University. She is a member of the California State Bar, the United States District Court for the Northern District of California, and the United States Court of Appeals for the Ninth Circuit.

William Sloan Coats is the executive partner in charge of the Palo Alto office of White & Case LLP. As an intellectual property attorney, Mr. Coats focuses his practice on cases involving software copyrights, patents, trademarks, and trade secret disputes for the software, electronics, and movie industries and bankruptcy issues. He represents leading business, computer, and entertainment hardware and software companies in complex intellectual property matters.

Mr. Coats has held various leadership positions within the American Bar Association's technology-related sections and divisions. He is currently the chair of the ABA Task Force on Biometrics and chair-elect of the Science and Technology Law Section and was a past chair of the Computer Law Division. Mr. Coats is also a member of the Delegation to the United Nations Commission on International Trade Law Working Group on Electronic Commerce.

Throughout his career, Mr. Coats has given many speeches and presentations and has published numerous articles on intellectual property issues in the computer, entertainment, and music industries. Most recently, Mr. Coats

gave a presentation titled "Investor Liability After *Grokster*" at the Fourth Annual Rocky Mountain Intellectual Property & Technology Institute Conference. He also gave a presentation on biometric technology at the Fifth Annual Global Privacy Symposium.

Mr. Coats is a member of the California State Bar, the U.S District Courts for the Northern, Central, Eastern, and Southern Districts of California, the U.S. Courts of Appeals for the Ninth Circuit, and the Federal Circuit and the U.S. Supreme Court.

Tarek Helou is an associate in Orrick, Herrington & Sutcliffe LLP's San Francisco office. He is the chairman of the ABA's Committee on Biometrics.

Mr. Helou's practice focuses on white-collar criminal investigations, securities enforcement actions, and intellectual property litigation. He spoke on a panel at the ABA's 2005 Summer Intellectual Property Law Conference. He earned a B.A. from Johns Hopkins University and a J.D. from New York University School of Law.

Taryn Lam is an associate in the Palo Alto office of White & Case LLP. Her practice focuses on intellectual property litigation, including patent, trade secret, and copyright litigation. Ms. Lam has assisted in the representation of high-technology clients in state, federal, and foreign courts.

Ms. Lam received her bachelor of arts degree from Pomona College and her juris doctor degree from the University of California, Berkeley. During law school, she served as an associate editor of the *Asian Law Journal*. She is a member of the California State Bar and the U.S. District Court for the Northern District of California. Ms. Lam is currently vice chair of the American Bar Association's Committee on Biometrics.

Contents

Chapter I

Introduction

*Tarek J. Helou**

I. Introduction

The use of biometric identifiers had been increasing before members of al-Qaeda hijacked four airliners on September 11, 2001. Government agencies had already required biometric identifiers to control access to some secure buildings and areas. Private companies had started to use biometric identifiers to facilitate retail payments. September 11 led to an increase in calls for the use of biometrics. Most planned new uses have sought to address security shortcomings.

In the near future, you will pay for things, go through airport security, and log onto your computer simply by scanning your iris, retina, or fingerprint. Biometrics are the most accurate form of identifiers and, when used properly, can greatly simplify life. However, biometrics raise new questions about personal privacy, surveillance, and the effects of government and corporate databases that register and hold fingerprint data and other biometric information. Despite these concerns, advocates in the government and private sector claim that the use of biometrics will enhance privacy and reduce identity theft by decreasing reliance on credit cards, Social Security numbers, and passwords, all of which can be lost or stolen easily. Biometrics also raise novel questions of intellectual property law, including who will own the copyrights to data related to or derived from your biometrics and who will have the right to use that data.

Like all technological advancements, biometrics must be used carefully. However, like all technological advancements, biometrics cannot be prohib-

* Tarek J. Helou is an associate at Orrick, Herrington & Sutcliffe, LLP, San Francisco.

ited from flourishing because of concerns over misuse. Society must adapt to technology because failing to do so is impossible and impedes the advancement of civilization.

A. What Are Biometrics?

Biometrics represent the measurement of any physiological characteristic or personal trait that is distinctive to an individual or a behavioral characteristic.[1] Colloquially, it has come to mean the measurement and matching of physiological characteristics for purposes of identification or verification. Physiological characteristics are unique identifiers because no two people—not even identical twins—have identical biometric measurements. In this sense, biometrics are more accurate than other forms of identification, even DNA testing.[2]

In practice, however, biometric data collection relies upon the creation of a template based on a person's unique characteristics. These characteristics include physical features, such as fingerprints, iris scans, and voice scans. They also include behavioral features, such as gait and handwriting. Therefore, because biometric identifiers use a template, they are *highly reliable but neither perfect nor unique.*

As opposed to being a consistently replicable string of data, such as a Social Security number, biometric samples differ with each recording. For example, the same fingerprint will generate a slightly different sample every time it is recorded. The differences are attributable to several factors, including dissimilar finger placement, poorly maintained collection devices, and even changes in weather conditions, such as humidity or temperature. Some biometrics, like fingerprints, retinal patterns, and iris patterns, are relatively stable and change only through time, injury, or disease. Others, such as facial and voice patterns, are inherently unstable and change frequently. Thus, they are more prone to disguise, manipulation, and incorrect readings.

To deal with these issues, biometric collection devices create algorithms based on user biometrics. A user's stored biometric and the biometric he or she presents to a biometric system would appear different because a small percentage of the biometric data changes with each placement in a biometric scanner. Thus, the biometric-based systems create algorithms that approximate the user's biometric. A biometric algorithm that was a unique identifier would never allow the wrong person to pass for someone (a false accep-

tance), but would also result in many instances in which an individual's biometric was not matched to the stored biometric (false rejections). By contrast, a system using a biometric algorithm that permits a match with decreased sensitivity will increase false acceptances but decreases false rejections. The use of two biometrics, although more costly and time-consuming, reduces false acceptances and false rejections.

B. Biometrics Are Not a Silver Bullet to Combat Terrorism or Identity Theft

Many people view the use of biometrics as a panacea to future terrorist attacks. This belief caused biometrics to leap to the forefront of national and international debates on security after September 11. This view persists because the use of biometric identifiers is often seen as a foolproof way to identify an individual or verify his or her identity. However, no method of verification or identification is foolproof and *no single technology or system—or group of them—can guarantee security.* Although biometric identifiers are not infallible, they can increase security significantly and they are the most accurate available form of identification.

Biometrics are not perfect and never will be. However, that does not mean that we should not implement better systems. The goal with biometrics, as with any other identification system, is improvement, not perfection.

C. A Description of the Different Types of Biometrics

Physiological biometrics, which are more common and generally more accurate than behavioral biometrics, include fingerprint scans, iris scans, retina scans, hand scans, and facial scans. Behavioral biometrics, which incorporate time and data based on user action, include voice recognition programs, keystroke recognition, and signature recognition. Biometrics can be as simple as recognizing a familiar face or as complicated as a computerized system that analyzes fingerprints and voices.

The most commonly used biometric systems are fingerprints, iris scans, face recognition, and hand geometry. These technologies vary not only in terms of their accuracy but also in the types of applications and facilities for which they are best suited.

1. *Physiological Biometrics*

a. Fingerprints

According to the International Biometric Group, fingerprints represent almost half the market share of biometric technologies. Fingerprints are most common in government settings because they are among the most accurate and least expensive of all biometrics. Fingerprints suffer from a high failure-to-enroll rate because some people cannot generate a clean fingerprint image and accuracy decreases with age. Fingerprint accuracy can be improved when multiple fingers from each individual are enrolled in a system. Fingerprint readers often use poroscopy, measure body heat, and incorporate pulse readers to ensure that the fingerprint offered is from a living person and it is a real finger (as opposed to a fake hand or a latent print). Fingerprints are also the least intrusive and most familiar of all biometrics.

b. Iris Scans

Systems that use iris scans represent approximately 10 percent of the market share of biometric technologies. Iris scans are the most accurate of all biometric technologies. Consequently, many high-security areas use iris scans. Iris scans are more intrusive than fingerprints, as the individual needs to place his or her eye very close to the reader, which also increases the amount of time for each scan. Iris scanners are becoming more powerful and are effective from increased distances. Iris scan systems are more expensive than other types of biometrics scanners.

c. Facial Recognition

Facial recognition systems represent approximately 10 percent of the market share of biometric technologies. One advantage of face recognition systems is that it can be easily confirmed by a system operator, such as a guard, by comparing a picture in a database with the individual's face. Face recognition systems are less intrusive than any biometric but are also less accurate and rely on several external factors, such as camera quality, facial position, facial expression, and other features such as facial hair or sunglasses.

d. Hand Geometry

Systems that use hand geometry represent approximately 10 percent of the market share of biometric technologies. Hand-geometry devices have a

higher false acceptance rate than fingerprint scanners. Like fingerprint readers, hand-geometry readers require little user training. Hand-geometry readers are relatively inexpensive.

2. Behavioral Biometrics

a. Voice Recognition

Voice or speech patterns represent a small percentage of the market share of biometric technologies. A person says specific words that the system records at enrollment. The system then prompts the person to say one or more of those words when the person is using the system. The system analyzes the speech pattern and determines whether the voice matches the prerecorded version of the words. Voice recognition systems are susceptible to changes in voices created by illness or background noise.

b. Keystroke Recognition

Keystroke recognition analyzes the way an individual types. Users enroll in a system by typing the same word or words several times. The system verifies the user by recognizing the distinctive rhythm a person uses while typing.

c. Signature Recognition

Signature recognition identifies an individual's handwritten signature by scrutinizing the unique way in which a signature is written. Signature verification is different from signature comparison. Signature comparison only examines how the signature looks. Signature verification assesses how the signature was created—instead of addressing the shape of the signature, it looks at changes in the shape, speed, stroke, pressure, and timing that occur during the act of signing.

D. Identification and Verification

The use of biometrics serves two closely related purposes, identification and verification. Identification systems perform "one-to-many" matches and verification systems perform "one-to-one" matches.