

The Practitioner's Guide to Biometrics

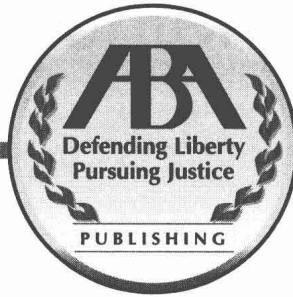
William Sloan Coats
Amy Bagdasarian
Tarek J. Helou
and Taryn Lam



ABA SECTION OF
SCIENCE & TECHNOLOGY LAW



Defending Liberty
Pursuing Justice



The Practitioner's Guide to Biometrics

William Sloan Coats

Amy Bagdasarian

Tarek Helou

and Taryn Lam



**ABA SECTION OF
SCIENCE & TECHNOLOGY LAW**



**Defending Liberty
Pursuing Justice**

Cover design by ABA Publishing

The materials contained herein represent the opinions and views of the authors and/or the editors, and should not be construed to be the views or opinions of the law firms or companies with whom such persons are in partnership with, associated with, or employed by, nor of the American Bar Association nor of the American Bar Association or the Section of Science & Technology Law unless adopted unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book and any forms and agreements herein are intended for educational and informational purposes only.

© 2007 American Bar Association. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. For permission contact the ABA Copyrights & Contracts Department, copyright@abanet.org or via fax at (312) 988-6030.

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

About the Editors	xi
--------------------------------	-----------

Chapter 1

Introduction	1
---------------------------	----------

Tarek J. Helou

I.	Introduction	1
A.	What Are Biometrics?	2
B.	Biometrics Are Not a Silver Bullet to Combat Terrorism or Identity Theft	3
C.	A Description of the Different Types of Biometrics	3
	1. Physiological Biometrics	4
	2. Behavioral Biometrics	5
D.	Identification and Verification	5
	1. Identification	5
	2. Verification	6
E.	Adjustment to Time-Induced Wear on Fingerprints	6
F.	Biometrics in Use Today	7
	1. National Security and Intelligence	7
	2. Law Enforcement	7
	3. Border Control and Immigration	8
	4. Commercial Applications	8
	5. Government Benefits	9
	6. Physical and Network Access	9
II.	Advantages of Biometrics	10
A.	Biometrics Are the Most Accurate Form of Identification	10
B.	Biometrics Are Unique Personal Identifiers	10
III.	What Has Driven Recent Increases in the Use of Biometrics?	11
A.	Demand for Better Identification and Verification	11
	1. National Security	11
	2. Identity Theft	11
B.	Increased Supply of Biometrics	12
IV.	Privacy Concerns	12
A.	Security Gains vs. Privacy Rights	12
B.	The Threat of a “Stolen Biometric” Has Been Exaggerated	13
C.	The Use of Biometrics as an Identification Tool for Law Enforcement and Intelligence Agencies	13

D. Database Linkage	13
1. Security and Commercial Improvements Are Directly Proportional to Database Linkage and Interoperability	13
2. Privacy Concerns Are Directly Proportional to Database Linkage and Interoperability	15
E. Cross-Border Privacy Issues	15
V. Conclusion	15

Chapter 2

Rethinking Data Protection Regimes to Enable Global Tracking and Prosecution of Terrorists 19

William Sloan Coats, Vickie L. Feeman, and Tarek J. Helou

I. Introduction	19
II. Use of Biometrics as a Means of Identifying Terrorists	21
A. Biometrics Are the Most Accurate Form of Identification	22
B. Biometrics Are Used More Often as Identifiers	22
C. Biometrics Will Enhance Security	23
D. The Use of Biometrics Abroad Will Help Fight Terrorism	23
E. Linked Databases Will Help Fight Terrorism	24
F. Biometrics Will Enable Security Gains Without Compromising Privacy Rights	25
1. Biometrics Will Help Combat Identity Theft	26
2. Racial Profiling Will Be Reduced as Investigators Focus on Suspicious Activity	26
3. Biometrics Can Be Used as Identification Tools for Law Enforcement and Intelligence Agencies	27
III. The Need for the EU to Amend Its Data Protection Directive	27
A. The EU Should Amend Article 26's "Public Interest" Exemption ..	29
1. Verbal Assurances from EU Nations That They Will Interpret the Exemption to Apply to American "Public Interest" Are Inadequate	29
2. Political Disagreements Hinder Data Sharing Between EU Members and the United States	30
B. The EU Should Expand Article 25's "Safe Harbor" Exemption Benefits to Apply to Financial Institutions	31
1. Financial Institution Biometric Databases Will Be the Largest in the Private Sector	31
2. Intelligence and Law Enforcement Agencies Will Increasingly Rely on Private-Sector Data Collection	32
IV. Conclusion	33

Chapter 3**United States Visitor and Immigrant Status Indicator****Technology Program 37***Michael R. Hoernlein*

I.	Introduction	37
II.	Persons Subject to US-VISIT	38
III.	US-VISIT Procedures	39
	A. Visa Application	40
	B. Entry Procedures	41
	C. Exit Procedures	41
IV.	Goals of US-VISIT	42
V.	Choice of Biometric Identifiers	43
VI.	How the Data Is Used/Privacy Issues	44
VII.	Conclusion	45

Chapter 4**Biometrics and National Identification Cards 49***Taryn Lam and Cynthia-Clare Martey*

I.	Introduction	49
II.	Worldwide Use of National Identification Cards	50
	A. Brazil	50
	B. Chile	50
	C. China	51
	D. Croatia	51
	E. Germany	51
	F. Israel	51
	G. Italy	51
	H. Pakistan	51
III.	Integration of Biometrics into National Identification Cards	52
	A. Countries Using Biometrics in Their National Identification Card Schemes	53
	1. Malaysia: MyKad Smart ID Card	53
	2. Hong Kong: A Case Study	54
	3. Australia: ePassport	55
	B. Countries Debating National Identification Card Schemes Including Biometrics	55
	1. The United States	56
	2. The United Kingdom	57
	3. Canada	58

IV. The Policy and Legal Debate Raised by the Use of Biometrics on National ID Cards 58

 A. Privacy 59

 B. Function Creep 60

 C. Discrimination 61

V. Conclusion 61

Chapter 5

Do Biometric Identifiers Make Us Safer? 67

Kyle D. Chen

I. Introduction 67

II. Effectiveness of Various Biometric Systems in Practice 69

 A. Facial Recognition 69

 B. Fingerprint Recognition 71

 C. Hand Geometry 72

 D. Iris Recognition 73

 E. Retina Recognition 74

 F. Voice Recognition 74

 G. Signature Recognition 75

III. Do Various Biometric Systems Make Us Safer? 75

IV. Conclusion 76

Chapter 6

Theft of Biometric Data: Implausible Deniability 79

Ian Johnson

Chapter 7

**Biometric Authentication from a Legal Point of View—
A European and German Perspective 87**

Astrid Albrecht

I. Introduction 87

II. The Different Aspects of Biometrics 88

III. Interoperability by Standardization 89

IV. Process of Biometric Identification 90

V. Data Security through Biometrics 92

VI. Security of Biometric Systems 93

VII. Security Infrastructures for Biometric Systems 93

VIII. Implications of Data Protection to Biometrics 94

 A. Legal Framework for Data Protection in the European Union 95

 1. Legal Basis in Europe 95

 2. Core Values of the EC Data Protection Directive 97

 3. Article 29 Data Protection Working Party 97

B. Data Protection in Germany Relating to Biometrics 99

 1. Right to Informational Self-Determination 99

 2. Biometric Data as Personal Data According to German
 Data Protection Law 100

 3. Purpose Limitation 102

 4. Materiality Theory 103

 5. Proportionality Principle 103

 6. Prohibition of Discrimination 104

 7. Biometric Data as Sensitive Data 104

 8. Biometrics and the Concept of Privacy-Enhancing
 Technologies 105

IX. Biometrics and Border Control 106

 A. European Development 106

 B. Biometrics with Regard to Personal Documents in Germany 109

 1. Amendments to the Acts Governing Passports and
 Identity Cards 109

 2. Data Protection and Security Provisions with Biometrics
 Enhanced Personal Documents 111

X. Authenticity in Legal Transactions Through Biometric Actions 112

 A. Functions of the Written Form and Importance of Handwritten
 Signature 113

 B. Peculiarities of Electronic Documents 115

 C. Certainty of Evidence Obtained Through a Signature in
 the Declaring Person’s Own Hand 118

 D. Biometric Methods and Legal Proof 120

 E. Facilitated Proof in the Use of Biometrics 121

XI. Trust-Building Options in the Law 127

 A. Standard Terms of Business: Liability Clauses and Duties of
 Skill and Care 127

XII. Employee Data Protection 129

XIII. Outlook 131

Chapter 8
Biometrics in the Private Sector: Trends and Case Studies 139

Rocky C. Tsai

I. Introduction 139

II. Network and Physical Access Security 140

III. Biometric Payment Systems 141

IV. Personal Data Protection 142

V. Travel 143

VI. Corporate Data Protection 143

VII. Standards and Commercial Adaptation 144

Chapter 9**The Application of Biometrics to Payment Verification 147***Taryn Lam*

I.	Introduction	147
II.	How Biometric Technology Can Be Used to Verify Payments	149
	A. Payment Verification	149
	B. Check Cashing	151
III.	The Benefits of Biometric Payment Systems	151
	A. Increased Sales	152
	1. Greater Customer Convenience and Satisfaction	152
	2. Faster Transaction Time	154
	3. More Effective Customer Loyalty Programs	155
	B. Cost Savings to Businesses	155
	1. Lower Transaction Costs	156
	2. Fewer Instances of Fraud	157
IV.	Current Implementation of Biometric Payments in the Retail Sector ..	158
V.	Conclusion	159

Chapter 10**Biometrics and Digital Rights Management 163***Chris Jay Hoofnagle*

I.	Biometrics Overview	163
	A. Creating and Using an Identity Database	164
	B. One-to-One Matching	164
	C. One-to-Many Matching	165
	D. Entering a New Person into the Database	165
II.	Fraud Will Not Be Eliminated Through Use of Biometrics	166
	A. There Are Too Many Practical Problems with Biometrics	166
	B. It Is Too Cost-Prohibitive to Use Biometrics on a Wide Scale	167
	C. Some People Will Be Unable to Enroll in Biometric Systems	167
	D. Collection of Information Creates New Threats to Privacy	168
	E. There Are Many Technical Problems with Biometrics	168
	1. Uniqueness of Biometric Data Is Affected by Time, Variability, and Data Collection	168
	2. Collecting Biometric Data Introduces Errors in the Data	168
	3. Increasing the Speed of Biometric Systems Can Introduce Error	169
III.	Systems Are Subject to Circumvention	169
IV.	Digital Rights Management and Privacy	170
V.	U.S. Law and Tradition Have Protected Privacy of Media Consumers ...	172

Chapter 11
Unintended Consequences of Biometrics 175
Todd Inskip and Theodore F. Claypoole

- I. Introduction 175
- II. What Are Companies Measuring? 177
- III. Why Is Biometric Information Collected? 179
 - A. Security Influence 180
 - 1. Positive Influence 181
 - 2. Negative Influence 182
 - 3. Example: Positive or Negative Influence? 183
 - B. Customer Service 183
 - C. Government 185
- IV. Current Trends That Will Predict the Future 186
 - A. Privacy Protection under the Current Law 186
 - B. American Privacy Model 187
 - C. Privacy and Security Practices 188
 - D. Law Enforcement and the Constitution 190
 - E. Proposals Affecting Biometrics 191
 - F. Business and Biometrics 192
 - G. Is the Legal System Ready? 192
- V. Living on the Fault Line—Biometric Issues That May Arise 195
 - A. Acceptance of Biometric Standards 195
 - 1. De Facto Standards versus Chosen Standards 198
 - B. Evidentiary and Procedural Issues 199
 - C. Database Issues 200
 - 1. Metabases—Government Participation 201
 - 2. Bleeding Data—Centralized versus Distributed Database 201
 - 3. Non-permissive Bleeding 202
 - D. Growth of Legal Protections 203
 - E. Government ID Cards/Default Cards 205
 - F. Collection Issues/Registration 205
 - 1. Notification 208
 - 2. Privacy Policy 209
 - 3. Request for Consent or Opt-In 209
 - 4. Reminders 210
 - 5. Opportunities 210
 - 6. Repeated Consents 210
 - 7. Extension 211
 - G. Other Issues 211
- VI. Summary 214

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.