

Biometrics: Identity Assurance in the Information Age
by John D. Woodward, Jr. et al.

Berkeley, California: McGraw-Hill/Osborne, 2003, ISBN 0-07-222227-1,
(Price \$ 49.99).

By Lia Burnham
J.D. Candidate
Suffolk University Law School

"The right to privacy is one of our most cherished freedoms. As society has grown more complex and people have become more interconnected in every way, we have had to work even harder to respect privacy, the dignity, and the autonomy of each individual... We must develop new protections for privacy in the face of new technological reality."¹

Introduction

The authors define biometrics as "life measurement", and further explain it as "methods of authentication based on physical or behavioral characteristics of an individual".² The technology of biometrics has inspired science fiction films in the past, and yet it is the reality of modern business.³ Although biometrics technology raises several legal questions, privacy stands out as the core concern.⁴ This review will focus primarily on the concept of trading privacy for security in a post-September 11th America.

¹ See page 197 (quoting President William J. Clinton in his commencement address at Morgan State University on May 18, 1997).

² See page 27.

³ See page 80 (discussing the voice recognition technology depicted in Stanley Kubrick's 1968 film *2001 Space Odyssey*). See *Id.* (comparing a speaker recognition system developed by Texas Instruments for the U.S. Air Force in 1977). Today, voice activated biometrics are utilized by Microsoft, Apple, AT&T, Lucent and Motorola. *Id.* at 85-86.

⁴ See generally Chapters 12 and 13 (discussing both privacy and religious considerations as the primary bases for legal challenges to biometric systems). *But see* page 231 (admitting the religious concerns "implicate" privacy issues). See also page 243-46 (formulating the international law arguments both for and against the use of biometrics).

College students at the University of Georgia, Pentagon employees, and Los Angeles County welfare recipients all submit to biometric scans on a regular basis.⁵ The University of Georgia uses a hand geometry scanner to control access to meal programs and dormitory rooms.⁶ The Pentagon uses an iris pattern biometric to ensure only employees use its gymnasium.⁷ Los Angeles County welfare recipients are fingerprinted to help curb welfare fraud.⁸ These entities and others report few complaints from the participants in their biometric programs.⁹ Perhaps they have not complained because they do not yet realize the extent of possible harm.¹⁰ Or perhaps they do not realize they are participants at all.¹¹

Background

Each of the authors brings direct experience in biometrics to this book.¹² John D. Woodward, Jr. has degrees in economics and law.¹³ He is the former operations officer for the Central Intelligence Agency, and has testified on biometrics before Congress.¹⁴ He has written numerous articles on biometrics, and authored two other books on the

⁵ See pages 284, 303, and 348.

⁶ See page 348.

⁷ See page 303.

⁸ See page 284.

⁹ See page 285 (finding most participants in Los Angeles County's welfare system did not feel "inconvenienced" by the fingerprint requirement). See also page 343 (noting that ING Direct Banking found very little concern about privacy when it started a fingerprint pilot program). But see page 285. (acknowledging one case was brought against the system in 2001, which upheld the fingerprinting biometric).

¹⁰ See page 324 (warning "the more trust we put in identification technology, the more rewarding fraud becomes").

¹¹ See pages 330-37 (noting the intense use of facial recognition biometrics by casinos). See also page 345 (discussing the voice verification biometric used by Charles Schwab)

¹² See "About the Author" page following copyright page.

¹³ *Id.*

¹⁴ *Id.*

subject.¹⁵ Today he is a senior analyst at the public policy research organization RAND.¹⁶ Nicholas M. Orlans has degrees in mathematics and architecture.¹⁷ He is the principal investigator and a lead engineer for MITRE experimentation in biometrics.¹⁸ Peter T. Higgins served at the Federal Bureau of Investigation as deputy assistant director in charge of IAFIS, the world's largest fingerprint automation project.¹⁹ He has degrees in theoretical math and computer science, and was in the Senior Intelligence Service of the Central Intelligence Agency.²⁰ Today he teaches biometrics at UCLA.²¹

The use of one's body as the ultimate computer password invokes the legal concept of privacy.²² Although not specifically mentioned in the U.S. Constitution, "the right of privacy is a fundamental personal right, emanating 'from the totality of the constitutional scheme under which we live'."²³ In Griswold v. Connecticut, 381 U.S. 479 (1965) the Court issued a landmark ruling when it held the right of privacy to be a fundamental personal right guaranteed to the people by the "penumbra" of the Ninth Amendment.²⁴ The Court struck down a Connecticut law forbidding the use of

¹⁵ *Id.* See generally John D. Woodward, Jr., et al., BIOMETRICS: A LOOK AT FACIAL RECOGNITION (RAND 2003); Katharine W. Webb, et al., ARMY BIOMETRIC APPLICATIONS: IDENTIFYING AND ADDRESSING SOCIOCULTURAL CONCERNS (RAND 2001).

¹⁶ See "About the Author" page following copyright page.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² See page 135 (referring to the phrase, "Your body as password").

²³ See Griswold v. Connecticut, 381 U.S. 479, 494 (1965) (Goldberg, J., concurring) (citing partially Poe v. Ullman, 367 U.S. 497, 521)

²⁴ See *Id.* at 484-86.

contraceptives because a governmental regulation may not "sweep unnecessarily broadly", thereby invading a relationship within the "zone of privacy".²⁵

The authors note that cases following *Griswold* expanded the concept of privacy to encompass new areas of law.²⁶ Breaking the zone of privacy into three distinct areas, the authors discuss each type of privacy as a separate legal hurdle over which biometrics must leap in order to be widely accepted in business.²⁷ The first form of privacy, physical, is protected under the Fourth Amendment's ban against unreasonable searches and seizures.²⁸ Physical privacy can be defined as freedom from contact or monitoring by others.²⁹ In *Thom v. New York Stock Exchange*, 306 F.Supp. 1002 (S.D.N.Y. 1969), the court held fingerprinting of employees is a mere means of identification, does not constitute an unreasonable search or seizure, and therefore does not violate privacy rights.³⁰

Decisional privacy is the second form addressed by the authors in examining the legal foundation for the use of biometric technology.³¹ The authors define decisional privacy as the freedom of choice in personal matters.³² *Roe v. Wade*, 410 U.S. 113 (1973) is the leading example of the Court's commitment to upholding decisional

²⁵ *See Id.* at 485.

²⁶ *See* page 219-20.

²⁷ *Id.* at 220.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *See Thom v. New York Stock Exchange*, 306 F. Supp. 1002, 1009 (1969) (comparing fingerprint identification to the invasiveness of submitting a photograph or signature to an employer).

³¹ *See* page 225.

³² *Id.*

privacy.³³ Since biometrics do not often invoke the concept of decisional privacy, the authors utilize a hypothetical situation to emphasize the way in which biometrics may infringe on this form of privacy in the future.³⁴ A state legislature could pass a law requiring all children attending private day care to submit to biometric scanning in the interest of finding missing children.³⁵ Some parents may invoke the concept of decisional privacy to prohibit the scanning of their child.³⁶ While not yet an issue, the authors advise that decisional privacy could become an important legal concern as biometrics become more widely used.³⁷

The authors define informational privacy, the third area of privacy discussed, as an individual's freedom to limit access to information about him or herself.³⁸

Informational privacy is the type most often implicated in biometric technologies, because for every biometric measurement taken, information about the supplier of the biometric is given.³⁹ For instance, if a person submits their fingerprints to gain access to a government facility, the computer can check several databases for criminal records.⁴⁰ The Court in Whalen v. Roe, 429 U.S. 589 (1977) found that a databank which matched the names of prescription drug buyers against particularly harmful prescription drugs did

³³ See Roe v. Wade, 410 U.S. 113, 153 (holding the "concept of personal liberty...is broad enough to encompass a woman's decision whether or not to terminate her pregnancy"). The Court elaborated that the privacy right only extended up until the point that the fetus became viable outside of the mother's womb. *Id.* at 164-65.

³⁴ See page 225.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ See page 221.

³⁹ See page 204-5 (admitting further use of biometrics will eventually lead to a "loss of individual autonomy").

⁴⁰ See page 55 (discussing the FBI automated fingerprint system IAFIS). Today, the FBI system takes approximately two hours to make a match or discount the individual. *Id.*

not violate the buyers' privacy rights.⁴¹ Since 1977, however, biometric technology has begun to infiltrate the market.⁴² Whether or not the legal rulings of the past can keep up with the technology of the future is yet to be determined.⁴³

Analysis

Having worked directly with many biometric programs, the authors are clearly proponents of the technology.⁴⁴ Their threshold concern for personal privacy is quickly overcome with a single presumption.⁴⁵ There is no real difference, the authors argue, between a police officer spotting a criminal in a crowd, and facial recognition software used to scan the Superbowl audience.⁴⁶ At first glance, this argument is convincing.⁴⁷ After all, biometric technology can be an effective law enforcement aid.⁴⁸ It can actually protect privacy by restricting access to medical files.⁴⁹ Viewed in this way, biometrics

⁴¹ See *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (arguing the safeguards inherent in any government database will protect the privacy of the individuals submitting their information).

⁴² See Chapter 16 (discussing sixteen biometric programs currently being used by state and local governments and the military). See also Chapter 18 (focusing on the casino industry, financial industry, and the retail industry as leading biometric users).

⁴³ See page 198 (acknowledging "technology is fast and the law is slow").

⁴⁴ See "About the Author" page following copyright page. See also page 326 (advocating the use of fingerprint biometric technology because despite the privacy concerns, the "technology and processes ...while not infallible, are mature and reliable."). See also page 334 (touting the successes of the casino industry in catching cheaters). The authors add that facial recognition technology can be instituted "for as little as \$675 per month". *Id.* at 335.

⁴⁵ See Chapter 14 (studying the Super Bowl Surveillance event in 2001).

⁴⁶ See page 248-50.

⁴⁷ *Id.*

⁴⁸ *Id.* See also page 252 (noting facial recognition software was implemented in more government agencies after the terrorist attacks of September 11, 2001).

⁴⁹ *Id.* at page 211.

are pioneering, useful and safe.⁵⁰ The problem is, then, not with the technology itself, but with the humans that tamper with it.⁵¹

The "human problem" manifests itself primarily in two different scenarios, both of which implicate the law of privacy.⁵² First, the authors discuss the concept of "function creep."⁵³ Basically, the government can gather data for one purpose, and eventually use it for another more invasive purpose.⁵⁴ For instance, Social Security numbers were originally supposed to be used for tax purposes only.⁵⁵ Today, they serve a wide range of functions, including obtaining credit cards and insurance.⁵⁶ In fact, the overuse of Social Security numbers has led to many cases of identity theft in recent years.⁵⁷ The authors also discuss a name database originally instituted for census purposes, which was eventually used to imprison 120,000 persons of Japanese descent during World War II.⁵⁸ In *Whalen*, when the Court reasoned database safeguards would

⁵⁰ *Id.*

⁵¹ *See Id.* at 9 (admitting if a biometric is "made by humans, it can be defeated by humans"). *See also* page 141 (discussing various techniques used to fool biometric devices including cadaver fingers and gelatin fingers).

⁵² *See* Chapter 12.

⁵³ *See* page 207 (quoting Justice Brandeis, in his dissenting opinion from *Olmstead v. United States*, 277 U.S. 438 (1928)). "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent...The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding." *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.* at page 207-8 (noting that originally the Social Security card had an advisory which said "Not for Identification").

⁵⁶ *Id.*

⁵⁷ *See page* 230 (discussing *In Re Crawford*, 194 F.3d 954 (9th Cir. 1999)). The plaintiff feared listing his Social Security number on documents of public record would make him vulnerable to identity theft. *Id.* The court held that his fear was outweighed by the government's need to provide public access to bankruptcy proceedings. *Id.* at 231.

⁵⁸ *Id.* at page 323.

protect the identities of prescription drug users, perhaps it did not recognize the danger of mission creep on the users' privacy interests.⁵⁹

The second way biometric technology can infringe upon privacy rights is by storing private medical information.⁶⁰ Ordinarily, databases use biometric information as a key, much like a computer password.⁶¹ Thus, a biometric can enable the user to enter a building or use a classified system.⁶² Biometrics, however, can also yield medical information as a byproduct of gaining entry into the system.⁶³ This information may be personal, embarrassing, or even unknown to the user herself.⁶⁴ For instance, retina scans may be able to disclose the existence of glaucoma and diabetes.⁶⁵ Fingerprints may be able to identify other diseases as well.⁶⁶ If the database retains this information, it may be accessed illegally by hackers, or used unscrupulously by those in a position of power.⁶⁷

⁵⁹ *Id.* at page 225-31. *But see Whalen*, 429 U.S. at 879 (admonishing that the court is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files").

⁶⁰ *Infra* note 65.

⁶¹ *Supra* note 22.

⁶² *See* page 303 (discussing the Pentagon's use of iris recognition technology and DoD Common Access Card for secure computer networks).

⁶³ *See* page 95.

⁶⁴ *Id.*

⁶⁵ *See* page 95 (noting glaucoma and diabetes affect the retina). *See also* page 90 (finding iris melanoma causes lesions on the iris and can be detected "during routine eye examinations"). *But see* page 98-9 (comparing retinal scans with the more invasive medical procedure called angiography). The authors contend that the retinal scan cannot find medical information because it is not as extensive of a scan as the angiography, and does not use dye. *Id.* In addition, the authors claim that since only a small part of the retina is stored in the computer, the medical information is safe. *Id.*

⁶⁶ *See* page 326, footnote 25 (admitting research has found fingerprints and footprints may yield information about chromosomal abnormalities such as Down's Syndrome).

⁶⁷ *See* page 376 (admitting that a major problem with the concept of a national ID system is that, "there is more information to reveal and hackers will be incentivized to break in"). *See also* page 207 (discussing function creep using the example of Japanese internment camps).

Conclusion

The recent events of September 11, 2001 have brought the concept of security to the forefront of the nation's conscience. Biometric technology can increase security for the nation as well as for individual businesses, however individuals should not have to sacrifice their privacy in exchange for the benefits of this new technology. This book is recommended for those interested in how biometrics are tested and perform for business. In addition, legal readers will find the last half of the book interesting, where the authors discuss privacy issues and new biometric technologies on the horizon.