

Index

• Numerics •

2D (two-dimensional) signature, 83
3D fingerprint image, 72–73
3D signature, 85–86

• A •

AAA (Triple A), 27, 66, 125–126, 269
accelerometers, 86, 189
acceptability, 15, 269
acceptance, false
 defined, 22
 False Acceptance Rate (FAR), 22, 69, 123, 124, 272
 with identical twins, 107
 iris scan eliminating, 94
 in stylus-movement dynamics, 81
access control, 269
access-control systems, 9–10, 121
accounting. *See* audit records
accuracy, 15, 269
administrative controls, 178, 269
Aladdin Knowledge Systems (company), 211
alarms, 266
algorithms, Daugman, 93, 191, 192
American National Standards Institute (ANSI), 128
antibody biometrics, 204–205
application attacks, 175
assets, 269
attacks. *See also* securing biometric systems;
 threats; vulnerabilities
 application, 175
 bypass, 20, 173, 270
 computer system, 173–174
 defined, 164, 269
 enrollment fraud, 20
 faked credentials, 171–172
 injection, 248
 man-in-the-middle, 167
 network, 174–175

 overview, 20, 170–171
 re-enrollment, 173
 replay, 20, 125, 171, 274
 social engineering, 170, 176, 274
 stolen credentials, 172
audit records
 defined, 30, 269
 regulatory requirements for, 125–126
 tamper-proof protection for, 30
authentication
 benefits of biometrics for, 245–246
 defined, 21, 27, 269
 described, 180
 failure, 59, 127, 238–239
 identification versus, 22, 27–28, 218
 logging and reporting system, 126–127, 246–247
 monitoring, continuous, 113
 multifactor, 27–28, 113, 273
 non-repudiation, 80, 246–247
 overview, 27–28
 regulatory requirements for, 125–126
authorization
 continuous monitoring, 113
 defined, 269
 overview, 28–29
 regulatory requirements for, 125–126
availability, 177, 270

• B •

backup plans, creating, 148–149
backups
 database, 149, 183
 hardware, 159
bacteria biometrics, 203–204
Banana Security (company), 212
barriers, physical, 263–267
behavior changes, 144–145
behavioral biometrics. *See also specific types*
 described, 12–13
 future technologies, 200–201

- benefits of biometrics
 - convenience of, 15–16
 - coolness of biometrics, 252
 - cooperation not required, 245–246
 - cost reduction, 250
 - elimination of password sharing, 16, 249
 - emergency identification, 251
 - high-throughput capabilities, 247
 - identity theft avoided, 251–252
 - organizational, 23–24
 - passwords versus, 247–248
 - physical location guaranteed, 246–247
 - regulation compliance, 250–251
 - reliable information, 15–16
 - unlosability of, 248–249
 - biometric basis
 - defined, 63
 - for DNA biometrics, 107
 - for facial biometrics, 95–97
 - for fingerprint biometrics, 64
 - for gait-recognition biometrics, 109–110
 - for hand-vein biometrics, 69–70
 - for iris scan, 93
 - for palm scans, 67–68
 - for retinal recognition, 90–91
 - for sonar/ultrasonic biometrics, 72
 - for speaker recognition biometrics, 103–105
 - for stylus-movement dynamics, 81–82
 - for typing dynamics, 112
 - biometric data storage, use and transmission standards, 128
 - biometric infrastructure, 176
 - biometric memory stick, 209
 - biometric systems. *See also* benefits of biometrics
 - behavioral types, 12–13, 200–201
 - benefits of, 15–16
 - characteristics of, 14–15
 - how they work, 13–14
 - implementing, 17–18
 - overview, 9–10
 - physiological types, 11–12
 - privacy issues, 18–19
 - protection for, 19–20
 - selecting, 16–17
 - terminology, 21–22
 - types of, 11–13
 - Biometrics Catalog, Web site, 223–224
 - BioPassword, Inc. (company), 112, 113
 - blind people, 24, 221
 - books, recommended, 184
 - border security. *See* ports of entry
 - brainwave biometrics
 - described, 115–116, 117
 - future technologies, 199
 - buddy punching, 250
 - budget, creating, 144
 - Burch, Frank (ophthalmologist), 92
 - business knowledge, 215–216
 - bypass attacks, 20, 173, 270
- C •
- cable protection, 181
 - cabling, 167
 - cameras
 - capabilities of, 194
 - infrared, 110, 111
 - video surveillance, 193, 266
 - car, driving sensors, 242
 - cardio-signature reader, 211
 - castle defense, 179
 - cell phones, 213–214, 241–242
 - Central Intelligence Agency (CIA), 41
 - CERT (Computer Emergency Response Team), 183
 - change management, 159–160, 270
 - Child Project, 94
 - choosing a biometric system. *See also* comparing biometric solutions; environment; testing a biometric system; vendor/manufacturer
 - analyzing your requirements, 130–131
 - biometric characteristics to consider, 14–15
 - cost considerations, 32, 126
 - determining requirements for, 128–129
 - determining users' needs, 24–25, 122
 - finding the simplest solution, 231–232
 - incorporating review feedback, 132–133
 - logging and reporting, 126–127, 181, 182, 246–247, 250
 - making the selection, 139–140
 - objectives for, 25–26
 - organizational needs, recognizing, 23–24
 - overview, 16–17, 30–31, 121
 - regulatory considerations, 33, 125–126

- reviewing your requirements, 132
- stakeholders input, 129–130
- surveying users for, 214, 227
- CIA (Confidentiality, Integrity, Availability), 19, 177, 270
- circumvention, 15, 270
- collectability, 15, 258, 270
- communicable disease, 145, 157
- communications
 - effective, 151
 - protecting, 180–181
 - with users, 149–152, 232
- comparing biometric solutions. *See also* selecting a biometric system
 - brainwave, 117
 - DNA, 117, 256–257
 - ear, 100
 - facial, 100
 - facial thermography, 100, 256–257
 - fingerprint, 73
 - gait-recognition, 117, 256–257
 - hand-vein, 73, 256–257
 - head-based, 100
 - iris scan, 100
 - odor biometrics, 117
 - palm scan, 73, 256–257
 - retinal scan, 100
 - sentence-structure, 117
 - signature, 87–88
 - sonar/ultrasonic, 73
 - speaker recognition, 117, 256–257
 - summary charts, 255–259
 - typing dynamics, 117, 256–257
- Computer Emergency Response Team (CERT), 183
- Computer Matching and Privacy Act of 1988, 19, 37–38, 270
- computer-network hosting facilities, 236–237
- computers
 - capturing a password, 111
 - fingerprint mouse, 211
 - laptops, 212–213
 - mouse-embedded palm-vein scanner, 71, 210–211
 - shared credentials of users, 10
 - system attacks, 173–174
 - weak passwords used for, 9–10
- Confidentiality, Integrity, Availability (CIA), 19, 177, 270
- configuration management, 160–161, 270
- constitutional rights
 - decisional privacy, 37
 - informational privacy, 37
 - physical privacy, 36
- contactless palm-vein imager, 210
- Content Scramble System (CSS), 25
- controls. *See also* securing biometric systems
 - administrative, 178, 269
 - control-failure modes, 177–179
 - defense in depth, 179, 270
 - detective, 177, 270
 - deterrent, 178, 271
 - preventive, 178, 273
- convenience, 26, 258
- cooperation, not required, 245–246
- costs. *See also* comparing biometric solutions
 - budget for, 144
 - enrollment, 126
 - hand-based biometrics, 73
 - monitoring system, 155
 - negotiating, 139
 - palm scans, 68
 - pricing potential solutions, 126
 - reducing, 250
 - testing a biometric system, 134
 - training, 126
- countermeasures, 258
- cow network, 124
- credentials
 - faked, 20, 171–172
 - for logging in, 181, 182
 - shared, 10
 - stolen, 170, 172
 - strong, 182
- credit-card data protection, 183, 241
- credit-card fingerprint scanner, 209–210
- credit-card theft, 251–252
- criminals, identifying, 51
- criteria for success
 - addressing users concerns, 226–227
 - allowing flexibility in planning, 229
 - business knowledge needs, 215–216
 - catching new problems quickly, 233
 - diplomacy skills, 215–216
 - finding the simplest solution, 231–232
 - maintaining the plan, 228
 - organizational needs and, 23–24, 225–226, 229–230

criteria for success (*continued*)
 overview, 136–137, 147
 researching biometric solutions, 230–231
 talking with users of biometric systems, 232
 for testing installations, 136–137
 users role in, 150, 227–228
 cryptographic hash, 18, 43, 272
 cryptographic signatures, 44
 CSS (Content Scramble System), 25
 customers. *See also* users
 manufacturers', 135
 understanding, 24–25

• D •

data. *See also* protecting biometric data
 credit-card data protection, 183, 241
 driver's licenses, 50–51
 irrelevant, ignoring, 58–59, 128
 mature data on already-installed systems,
 134–135
 storage, use and transmission standards,
 128
 tainted, 57
 data breach disclosure laws/security-breach
 laws, 52–54
 Data Protection Directive (Directive 95/46/
 EC), 55–56, 270
 database
 backups, 149
 vulnerabilities, 168
 database-management systems (DBMSs), 168,
 182
 Daugman algorithms, 93, 191, 192
 Daugman, John (physicist), 191, 224
 decisional privacy, 37
 decryption, 270
 defense in depth, 179, 270
 deoxyribonucleic acid (DNA)
 described, 106–107, 270
 of identical twins, 107
 Department of Justice, U.S., 37, 220
 detective controls, 177, 270
 deterrent controls, 178, 271
 devices, biometric. *See also* scanners/
 readers; tools used in biometrics
 physical vulnerabilities of, 167
 protecting, 180

digital signature, 271
 digitizer, 83
 diplomacy skills, 215–216
 Directive 95/46/EC (Data Protection
 Directive), 55–56, 270
 disabilities, users with, 221–222
 disaster-recovery planning, 165, 183
 disease, communicable, 145, 157
 disinfectants for cleaning, 157
 DNA biometrics
 biometric basis for, 107
 comparisons, 117, 256–257
 defined, 271
 drawbacks of, 15, 16, 107, 108
 future technologies, 196–197
 practical considerations, 107–108
 privacy concerns, 197
 uses for, 109
 DNA (deoxyribonucleic acid)
 described, 106–107, 270
 of identical twins, 107
 door lock, 10, 29
 driver's licenses, 50–51
 driving sensors for cars, 242
 dumpster diving, 176
 DVD movie, piracy protection, 25

• E •

ear recognition biometrics
 comparisons, 100, 256–257
 described, 98–99, 271
 future technologies, 194–195
 e-commerce data, protecting, 179
 education/training
 cost considerations, 126
 defined, 274
 for testing staff, 137–138
 users, 17, 137–138, 152–153
 EER (equal error rate), 271
 Elastic Bunch Graph Matching (EBGM), 96,
 271
 electrical field biometrics, 202
 electroencephalographs (EEGs), 115
 Electronic Frontier Foundation (EFF), 218–219
 Electronic Patient Health Information (EPHI),
 54, 271
 electronic signature, 79, 271

e-mail, acceptable use policies, 115
 emergency identification, 251
 employees/staff. *See also* users
 project manager, 142–143, 146
 safety of, 261
 as stakeholders, 129–130
 training, 137–138
 workloads, reducing, 250
 encryption, 180–181, 271
 enrollment. *See also* Failure To Enroll (FTE)
 cost considerations, 126
 defined, 78, 271
 fraud, 20, 271
 of users, 13, 138
 entryway access, 235–236
 environment. *See also* selecting a biometric system
 accuracy and “F”-rate requirements,
 determining, 123–124
 logging and reporting, 126–127, 246–247
 physical attributes of, 123
 pricing potential solutions, 126
 regulatory requirements, 125–126
 speaker recognition affected by, 104–105
 standards and interoperability, 128
 user privacy concerns, 127–128
 EPHI (Electronic Patient Health Information),
 54, 271
 error rates
 Equal Error Rate (EER), 124
 Failure To Acquire (FTA), 77, 81, 272
 Failure To Enroll (FTE), 77–78, 81, 123, 272
 False Acceptance Rate (FAR), 22, 69, 123,
 124, 272
 False Rejection Rate (FRR), 22, 69, 123–124,
 272
 ethical issues. *See also* privacy
 controlling how your biometrics are used,
 58
 failure to authenticate, understanding, 59
 irrelevant data, ignoring, 58–59, 128
 tracking individuals’ activities, 57–58
 European Union (EU)
 ports of entry, 56
 privacy statute, 54–56
 Web site, 55
 Executive Order 12333, 19, 39–41, 271
 eye-based biometrics. *See* iris scan; retinal scan

• F •

facial biometrics. *See also* facial thermography
 biometric basis for, 95–97
 comparisons, 100
 defined, 271
 facial photographs fooling, 172
 future technologies, 193
 laptop facial recognition, 212
 overview, 12, 94–95
 practical considerations, 97
 uses for, 97–98
 facial thermography
 comparisons, 100, 256–257
 defined, 272
 future technologies, 193–194
 overview, 99–100
 fail closed situation, 178–179, 272
 fail open situation, 178–179, 272
 failure
 control-failure modes, 177–179
 fault management for, 154–156
 fingerprint biometrics, 239
 signature biometrics, 77, 239
 software, 183
 Failure To Acquire (FTA), 77, 81, 272. *See also*
 signature biometrics
 failure to authenticate. *See also*
 authentication
 described, 127
 reasons for, 238–239
 understanding, 59
 Failure To Enroll (FTE). *See also* enrollment;
 signature biometrics
 described, 77–78, 272
 importance of, 123
 in stylus-movement dynamics, 81
 fake hands, 172
 faked credentials, 20, 171–172
 false acceptance
 defined, 22
 with identical twins, 107
 iris scan eliminating, 94
 in stylus-movement dynamics, 81
 False Acceptance Rate (FAR)
 defined, 22, 272
 determining, 123, 124
 hand-vein biometrics reducing, 69

- false rejection. *See also* False Rejection Rate (FRR)
 - described, 22
 - iris scan eliminating, 94
 - reasons for, 59
 - in stylus-movement dynamics, 81
- False Rejection Rate (FRR)
 - defined, 22, 272
 - determining, 123–124
 - hand-vein biometrics reducing, 69
 - reducing, 123–124
- fault management, 154–156
- federal and state laws, U.S.. *See also* legal issues
 - data breach disclosure laws, 52–54
 - Electronic Patient Health Information (EPHI), 54, 271
 - overview, 46–47
- feedback, review, 132–133
- findBIOMETRICS.com, 222
- fingerprint biometrics. *See also* fingerprint scanners
 - biometric basis for, 64
 - comparisons, 73, 256–257
 - compromised/failure, 66–67, 239
 - concerns about, 18
 - described, 11
 - fingerprint mouse, 211
 - future improvements, 185–187
 - live versus dead subjects for, 71
 - practical considerations, 64–65
 - protection for, 19, 43
 - stored as cryptographic hash, 18, 43
 - uses for, 48–49, 66–67
 - wearing gloves and, 24–25
- fingerprint scanners
 - credit-card fingerprint, 209–210
 - described, 272
 - types of, 64–65
- fingerprints
 - 3D image of, 72–73
 - described, 63, 272
 - gummy, 171
 - misappropriation of, 64
 - sanding off, 25
- firmware updates, 159
- flash drives, 213–214
- flexibility, allowing, 229
- flexion creases, 67
- fMRI (functional magnetic resonance imaging), 115
- forgery
 - fingerprint, 15
 - signing a signature, 81–82
- “F”-rate requirements, 123–124
- FRR (False Rejection Rate)
 - defined, 22, 272
 - determining, 123–124
 - hand-vein biometrics reducing, 69
 - reducing, 123–124
- FTA (Failure To Acquire), 77, 81, 272. *See also* signature biometrics
- FTE (Failure To Enroll). *See also* enrollment; signature biometrics
 - defined, 272
 - described, 77–78
 - importance of, 123
 - in stylus-movement dynamics, 81
- Fujitsu Laboratories (company), 210
- functional magnetic resonance imaging (fMRI), 115
- future technologies
 - behavioral biometrics, 200–201
 - brainwave biometrics, 199
 - DNA biometrics, 196–197
 - ear recognition biometrics, 194–195
 - facial biometrics, 193
 - facial thermography, 193–194
 - fingerprint biometrics, 185–187
 - gait-recognition biometrics, 197–198
 - hand-vein biometrics, 187–188
 - improvements, 185–200
 - iris scan, 191–192
 - linguistic analysis, 198–199
 - new, 200–205
 - odor biometrics, 200, 205
 - palm scan, 185–187
 - physical properties biometrics, 201–205
 - retinal scan, 190–191
 - sentence-structure biometrics, 198–199
 - signature biometrics, 188–189
 - speaker recognition, 195–196
 - typing dynamics, 198
 - ultrasonic/sonar biometrics, 187–188

• G •

gait-recognition biometrics
 biometric basis for, 109–110
 comparisons, 117, 256–257
 described, 13, 109, 272
 drawbacks of, 15
 future technologies, 197–198
 as kinematic biometrics, 203
 misuse of, 58
 practical considerations, 110
 uses for, 110–111

game-playing skills, 201

Gattaca (film), 108

gloves, 24–25, 230

Goldstein, Isidore (scientist), 90

government biometric projects
 biometric passports, 44
 identification system for special jobs, 49–50
 identification system for U.S. citizens, 50–51
 privacy issues, 43–46
 REAL ID, 50–51, 274

Gula, Sharbat (Afghan woman), 48, 217–218

gummy fingerprints, 171

• H •

hand-based biometrics, comparisons, 73. *See also specific types*

hand-sanitizer stations, 157

hand-vein biometrics. *See also palm scan*
 biometric basis for, 69–70
 comparisons, 73, 256–257
 contactless palm-vein imager, 210
 described, 11, 69, 272
 future technologies, 187–188
 mouse-embedded palm-vein scanner, 71, 210–211
 practical considerations, 70–71
 uses for, 71

handwriting. *See signature biometrics*

hard drives, portable, 213–214

hardware
 backups, 159
 failure, 183
 need for, 132

updates, 158
 upgrades to, 161

hash, 18, 32, 272

head and neck, illustration, 105

head-based biometrics. *See also specific types*
 comparisons, 100
 psychological components, 89

Health Insurance Portability and Accountability Act (HIPAA), 42, 125, 222, 272

health issues
 biometrics showing, 128, 190–191
 communicable disease, 157–158

healthcare
 Electronic Patient Health Information (EPHI), 54, 271
 environments, 122

Heisenberg, Werner (scientist), 86–87

helpdesk, 155–156, 250

heredity, 104–105

high-security hosting, 236–237

high-throughput identification systems, 247

Homeland Security Presidential Directive 12 (HSPD-12), 50, 272

• I •

IBG (International Biometric Group), 135

ICDRI (International Center for Disability Resources on the Internet), 221–222

icons used in this book, 4

identification
 authentication versus, 22, 27–28, 218
 biometrics' convenience for, 15–16, 245–246
 defined, 22, 273
 driver's licenses, 50–51
 emergency, 251

identification system, U.S.
 criminals, identifying, 51
 ID cards for special jobs, 49–50
 protections against misuse, 51–52
 REAL ID, 50–51, 274

identity theft, 251–252

IEC (International Electrotechnical Commission), 128

image-only signature biometrics, 12, 76–77, 79–80

- implementing a biometric system. *See also*
 - maintaining a biometric system; testing a biometric system
 - backout plans for, 148–149
 - building a plan for, 18, 142–144
 - communicating with users about, 149–152
 - executing the plan, 144–146
 - mid-course corrections, 146
 - overview, 17–18, 141–142
 - phasing the system in, 148
 - pilots and tests, running, 146–148
 - project management, 145–146
 - publishing information for users, 156–157
 - training/educating users, 17, 152–153
 - user issues, dealing with, 153
 - industry data, 135–136
 - information
 - health-care, 54, 128
 - irrelevant data, ignoring, 58–59, 128
 - personal, 54
 - Personally Identifiable Information (PII), 273
 - public, 41
 - published for users, 156–157
 - security guidelines, 183
 - sensitive, 41–42
 - surveying users for, 214, 227
 - information security management, 183
 - informational privacy, 37, 273
 - infrared camera, 110, 111
 - infrared imaging techniques, 99–100
 - injection attack, 248
 - Inmate Recognition and Identification System (IRIS), 94
 - installations, testing, 136–139
 - integrity, 177, 273
 - International Biometric Group (IBG), 135
 - International Center for Disability Resources on the Internet (ICDRI), 221–222
 - International Electrotechnical Commission (IEC), 128
 - interoperability, 128
 - Intranets, 156–157
 - Iridian Technologies, 92
 - iris, 92, 93
 - IRIS (Inmate Recognition and Identification System), 94
 - iris photographs, 172
 - iris scan
 - benefits of, 91
 - biometric basis for, 93
 - comparisons, 100, 256–257
 - described, 11–12, 273
 - example of use, 48, 217–218
 - future technologies, 191–192
 - iris mouse, 211
 - medical diagnostic tests using, 41–42
 - patents on, 92
 - practical considerations, 93–94
 - United Arab Emirates (UAE) using, 45, 94
 - iris scanner, 273
 - IrisCodes, 94
 - irrelevant data, ignoring, 58–59, 128
 - (ISC)² Global Workforce Survey, 1
 - ISO 17799 and ISO 27001, 183
- **K** •
- keycards, lost, 10
 - keypad, 236
 - keystroke dynamics
 - biometric basis for, 112
 - comparisons, 117, 256–257
 - described, 13, 111, 275
 - future technologies, 198
 - practical considerations, 112–113
 - uses for, 113–114
 - kinematic biometrics, 203
- **L** •
- laptops, 212–213
 - law enforcement, 68–69, 238
 - LDA (Linear Discriminant Analysis), 96–97, 273
 - legal issues. *See also* federal and state laws, U.S.; privacy laws
 - biometric ID cards for special jobs, 49–50
 - biometric identification system, U.S.
 - citizens, 50–51
 - data breach disclosure laws/security-breach laws, 52–54
 - European law, 54–56
 - laws in other countries, 56–57
 - need for privacy laws, 60
 - passport and port of entry, 47–49

Lenovo (company), 212
 life, proof of, 15, 192, 274
 Linear Discriminant Analysis (LDA), 96–97, 273
 linguistic analysis
 comparisons, 117
 described, 114–115
 future technologies, 198–199
 loading dock entry, 176
 locking users out, 155–156
 logging and reporting. *See also* passwords
 buddy punching, 250
 login credentials, securing, 181, 182
 non-repudiation, 246–247
 system for, 126–127

● **M** ●

magnetoencephalography (MEG), 115
 maintaining a biometric system. *See also*
 securing biometric systems
 change management, 159–160
 cleaning and maintenance, 145, 157
 configuration management, 160–161, 270
 firmware updates, 159
 hardware updates, 158
 monitoring system, 154–155
 software updates, 14, 158
 updating the data, 14
 upgrades, 161
 malware, 240–241
 management
 change, 159–160
 configuration, 160–161, 270
 fault, 154–156
 information security, 183
 project, 145–146
 risk, 216
 manager, project, 142–143, 146
 man-in-the-middle attack, 167
 manmade threats, 166
 manufacturer/vendor. *See also* on-site
 testing; selecting a biometric system
 choosing, 139–140
 determining biometric requirements and,
 131
 following up with, 140
 on-site testing through, 134–139
 reference contacts for, 133–134

 stability and support potential of, 139
 Web site resource, 222
 maturity, 258
 McCurry, Steve (photographer), 58, 217
 medical information, confidential, 128
 medical institutions, U.S., 114
 MEG (magnetoencephalography), 115
 memory stick, biometric, 209
 microbe biometrics, 203–204
 military installations, 91
 misuse of biometric data, 51–54
 monitoring, continuous, 113
 monitoring system, 154–155
 Moore's Factor, 258
 mouse, fingerprint or iris, 211
 mouse-embedded palm-vein scanner, 71,
 210–211
 multifactor authentication, 27–28, 113, 273
 multimodal biometrics, 99, 273

● **N** ●

National Biometric Security Project (NBSPP),
 135–136, 219
National Geographic (magazine), 48, 217–218
 National Institute of Standards and
 Technology (NIST), 183, 191, 220–221
 natural threats, 165–166
 neighborhood watch, biometric, 243
 NetNanny (company), 111, 112
 network
 attacks, 174–175
 resources, 132
 securing access, 181
 vulnerabilities, 167
 NIST (National Institute of Standards and
 Technology), 183, 191, 220–221
 non-genetic chemical biometrics, 203–205
 non-repudiation, 80, 246–247

● **O** ●

odor biometrics, 116, 117, 200, 205
 on-site testing. *See also* selecting a biometric
 system; testing a biometric system;
 vendor/manufacturer
 contacting manufacturer's customers, 135
 industry data on, 135–136

- on-site testing (*continued*)
 - installations for, 136–139
 - obtaining data on already-installed systems, 134–135
 - operating-system vulnerabilities, 167
 - optical fingerprint readers, 65
 - Organisation for Economic Cooperation and Development (OECD), 56
 - organizational needs
 - identifying, 23–24
 - importance of, 229–230
 - meeting, 225–226
- *p* ●
- Palm Beach International Airport, 98
 - palm scan. *See also* hand-vein biometrics
 - biometric basis for, 67–68
 - comparisons, 73, 256–257
 - contactless palm-vein imager, 210
 - costs of, 68
 - future technologies, 185–187
 - practical considerations, 68
 - scanners for, 64–65, 209–210, 273
 - uses for, 68–69
 - passports, biometric, 44, 270
 - passwords. *See also* logging and reporting
 - disadvantages of, 247–248
 - guessing, 174
 - sharing, 16, 111, 249
 - weak, 9–10
 - Payment Card Industry Data Security Standard (PCI DSS), 183
 - PCA (Principal Components Analysis), 96, 273
 - pen
 - with accelerometer, 86
 - holding, 85
 - performance, 15, 273
 - Performance and Standards Conformance, 136
 - permanence, 14, 258, 273
 - personal information, 54
 - Personally Identifiable Information (PII), 273
 - PET (Positron Emission Tomography), 115
 - physical privacy, 36
 - physical properties biometrics
 - described, 201
 - electrical field, 202
 - general kinematic, 203
 - non-genetic chemical, 203–205
 - skeletal structure, 202
 - physical security. *See also* securing biometric systems
 - alarms and video surveillance, 266
 - biometric systems controlling, 268
 - general principles, 261–263
 - information security versus, 262
 - physical barriers as, 263–267
 - physical damage, 262
 - preventive measures, 266
 - reacting to attacks, 267
 - sabotage, 262
 - safety of employees, 261
 - sightlines, 264
 - vandalism, 262
 - physiological biometrics, 11–12. *See also specific types*
 - PII (Personally Identifiable Information), 273
 - pilots and tests, running, 146–148
 - planning
 - backout plans, 148–149
 - building a plan, 18, 142–144
 - disaster-recovery, 165, 183
 - executing the plan, 144–146
 - flexibility allowed in, 229
 - maintaining the plan, 228
 - project manager for, 142–143, 146
 - portable hard drives, 213–214
 - port-of-entry identification, 237
 - ports of entry
 - EU nations, 56
 - United States, 47–49
 - Positron Emission Tomography (PET), 115
 - power plants, 91
 - preventive controls, 178, 273
 - Principal Components Analysis (PCA), 96, 273
 - privacy. *See also* ethical issues; legal issues
 - constitutional protections for, 36–37
 - DNA biometrics and, 197
 - European statute on, 54–56
 - health-care information, 54, 271
 - informational, 37
 - invasion of, 145, 239–240
 - irrelevant data, ignoring, 58–59, 128
 - maintaining a healthy balance, 45–46
 - managing concerns about, 60

- overview, 18–19, 42–43
 - protection against misuse, 51–54
 - sensitive information and, 41–42
 - statutory protections for, 37–39
 - tainted biometric data and, 57
 - U.S. government biometric projects and, 43–46
 - users concerns, 127–128, 226–227
 - privacy laws
 - Computer Matching Privacy Act of 1988, 19, 37–38, 270
 - Electronic Patient Health Information (EPHI), 54, 271
 - Executive Order 12333, 19, 39–41
 - need for, 60
 - overview, 18–19
 - Privacy Act of 1974, 19, 37, 274
 - problems, catching quickly, 233
 - productivity loss, 126
 - project management, 145–146
 - project manager, 142–143, 146
 - proof of life, 15, 192, 274
 - protecting biometric data. *See also* data; privacy; securing biometric systems
 - CIA (Confidentiality, Integrity, Availability), 19, 177, 270
 - constitutional protections, 36–37
 - misuse prevention, 51–54
 - overview, 19–20, 42–43
 - statutory privacy protections, 37–39
 - public information, 41
 - publications
 - books, recommended, 184
 - National Geographic*, 217–218
 - for users, 156–157
 - pupil, 274
- R •**
- readers/scanners. *See also* tools used in biometrics
 - cardio-signature, 211
 - contactless palm-vein imager, 210
 - credit-card fingerprint, 209–210
 - disinfectants for cleaning, 157
 - embed in objects, 241
 - fingerprint, 64–65, 272
 - hand-vein, 70
 - iris, 273
 - live versus dead subjects for, 71
 - mouse-embedded palm-vein, 71, 210–211
 - optical fingerprint, 65
 - palm print, 64–65, 209–210, 273
 - physical vulnerabilities of, 167
 - protecting, 180
 - retina, 274
 - thermoelectric, 65
 - updating, 158–159
 - reading skills, 201
 - REAL ID, 50–51, 274
 - record, 38
 - recorded voice, 172
 - re-enrollment attacks, 173
 - references, vendor/manufacturer, 133–134
 - Regan, Ronald (U.S. President), 39
 - regulatory requirements. *See also* requirements for biometric system
 - for authentication, authorization, and accounting (AAA), 125–126
 - complying with, 250–251
 - determining biometric needs and, 131
 - selecting a biometric system and, 33, 125–126
 - rejection, false
 - described, 22
 - False Rejection Rate (FRR), 22, 69, 123–124, 272
 - iris scan eliminating, 94
 - reasons for, 59
 - in stylus-movement dynamics, 81
 - reliability, 258
 - remote access, 176
 - repairs and replacement scenarios, 156
 - replay attacks, 20, 125, 171, 274
 - reporting and logging. *See also* passwords
 - buddy punching, 250
 - login credentials, securing, 181, 182
 - non-repudiation, 246–247
 - system for, 126–127
 - requirements for biometric system. *See also* regulatory requirements
 - analyzing, 130–131
 - defined, 274
 - determining, 128–129
 - reviewing, 132
 - retina, 90–91, 274
 - retina scanner, 274

- retinal scan
 - biometric basis for, 90–91
 - comparisons, 100, 256–257
 - described, 12, 91
 - drawbacks of, 15
 - failing to authenticate, 42
 - future technologies, 190–191
 - limitations of using, 92
 - medical diagnostic tests using, 41–42
 - practical considerations, 91
 - review feedback, 132–133
 - risk
 - biometric-related, 144–145
 - defined, 164
 - management, 216
 - road apple, 176
- S ●
- sabotage, 180, 262
 - SANS institute, Web site, 184
 - scanners/readers. *See also* tools used in
 - biometrics
 - cardio-signature, 211
 - contactless palm-vein imager, 210
 - credit-card fingerprint, 209–210
 - disinfectants for cleaning, 157
 - embed in objects, 241
 - fingerprint and palm-print, 64–65, 272
 - hand-vein, 70
 - iris, 273
 - live versus dead subjects for, 71
 - mouse-embedded palm-vein, 71, 210–211
 - mouse-embedded palm-vein scanner, 71, 210–211
 - optical fingerprint, 65
 - palm print, 64–65, 209–210, 273
 - physical vulnerabilities of, 167
 - protecting, 180
 - retina, 274
 - thermoelectric, 65
 - updating, 158–159
 - schedule, for implementation, 144
 - securing biometric systems. *See also* attacks;
 - controls; physical security; threats;
 - vulnerabilities
 - attacks, typical, 170–176
 - basic defenses, 177–179
 - biometric applications protection, 182
 - biometric data protection, 182–183
 - biometric device protection, 180
 - books, recommended, 184
 - communications protection, 180–181
 - defense in depth, 179, 270
 - fail closed situation, 178–179, 272
 - fail open situation, 178–179, 272
 - physical security versus, 262
 - protecting servers, 181
 - security information resources, 183–184
 - security breach laws, 52–54
 - security guards, 236
 - security patches, 181
 - selecting a biometric system. *See also*
 - comparing biometric solutions;
 - environment; testing a biometric system;
 - vendor/manufacturer
 - analyzing your requirements, 130–131
 - biometric characteristics to consider, 14–15
 - cost considerations, 32, 126
 - determining requirements for, 128–129
 - determining users' needs, 24–25, 122
 - finding the simplest solution, 231–232
 - incorporating review feedback, 132–133
 - logging and reporting, 126–127, 181, 182, 246–247, 250
 - making the selection, 139–140
 - objectives for, 25–26
 - organizational needs, recognizing, 23–24
 - overview, 16–17, 30–31, 121
 - regulatory considerations, 33, 125–126
 - reviewing your requirements, 132
 - stakeholders input, 129–130
 - surveying users for, 214, 227
 - Senior Safety Net, 94
 - sentence-structure biometrics
 - comparisons, 117
 - described, 114–115
 - future technologies, 198–199
 - server
 - malware on, 240–241
 - physical vulnerabilities of, 167
 - protecting, 181
 - sharing passwords, 16, 111, 249
 - signature biometrics. *See also* Failure To Enroll (FTE)
 - accelerometers used in, 86, 189
 - biometric basis for, 76–77

- cardio-signature reader, 211
- comparisons, 87–88, 256–257
- defined, 274
- electronic versus digital signatures, 79
- Failure To Acquire (FTA), 77, 81, 272
- failures, 77–78, 239
- future technologies, 188–189
- Heisenberg’s Uncertainty Principle applied to, 86–87
- image-only, 12, 76–77, 79–80
- overview, 12, 75–76
- practical considerations, 77–79
- speed of signing, 81–82
- stroke order and direction, 82
- stylus-movement dynamics, 12, 80–83
- stylus-pressure dynamics, 12, 84–86
- signature pads, electronic, 78
- Simon, Carleton (scientist), 90
- skeletal structure biometrics, 202
- social engineering, 170, 176, 274
- software
 - attacks, 175
 - for biometrics system, 132
 - failure, 183
 - firmware updates, 159
 - malware, 240–241
 - protecting, 182
 - updates, 14, 158
 - vulnerabilities, 168–169
- sonar/ultrasonic biometrics
 - biometric basis for, 72
 - comparisons, 73
 - defined, 274, 275
 - fingerprint, 65
 - future technologies, 187–188
 - overview, 71–72
 - practical considerations, 72–73
 - uses for, 73
- speaker recognition biometrics. *See also* voice
 - biometric basis for, 103–105
 - comparisons, 117, 256–257
 - described, 102, 274
 - future technologies, 195–196
 - heredity and environment’s influence, 104–105
 - practical considerations, 105–106
 - speech recognition versus, 103
 - voice recognition, 13, 27, 102, 275
- speech. *See also* speaker recognition
 - biometrics; voice
 - recognition, 103
 - samples, capturing, 105–106
 - translating into text, 27
- staff/employees. *See also* users
 - project manager, 142–143, 146
 - safety of, 261
 - training, 137–138
 - workloads, reducing, 250
- stakeholders, 129–130. *See also* staff/employees; users
- statutory privacy protections, 37–39
- stolen credentials, 170, 172
- storage of biometric data, 128
- stroke order and direction, 82
- stylus, 274
- stylus-movement dynamics
 - biometric basis for, 81–82
 - described, 12
 - practical considerations, 83
 - uses for, 83
- stylus-pressure dynamics
 - defined, 12
 - overview, 84–85
 - practical considerations, 85
 - uses for, 85–86
- subject uniqueness, 258
- success criteria
 - addressing users concerns, 226–227
 - allowing flexibility in the plan, 229
 - business knowledge needed for, 215–216
 - catching new problems quickly, 233
 - criteria for, 136–137, 147
 - diplomacy skills for, 215–216
 - finding the simplest solution, 231–232
 - maintaining the plan, 228
 - organizational needs and, 23–24, 225–226, 229–230
 - researching biometric solutions, 230–231
 - talking with users of biometric systems, 232
 - for testing installations, 136–137
 - users role in, 150, 227–228
- Super Bowl (2001), Florida, 97–98
- surveillance video, 193, 266
- surveying users, 214, 227
- system attacks, 173–174
- system of records, 38

• T •

- tailgating, 176
- tainted biometric data, 57
- technologies, future
 - behavioral biometrics, 200–201
 - brainwave biometrics, 199
 - DNA biometrics, 196–197
 - ear recognition biometrics, 194–195
 - facial biometrics, 193
 - facial thermography, 193–194
 - fingerprint biometrics, 185–187
 - gait-recognition biometrics, 197–198
 - hand-vein biometrics, 187–188
 - improvements, 185–200
 - iris scan, 191–192
 - linguistic analysis, 198–199
 - new, 200–205
 - odor biometrics, 200, 205
 - palm scan, 185–187
 - physical properties biometrics, 201–205
 - retinal scan, 190–191
 - sentence-structure biometrics, 198–199
 - signature biometrics, 188–189
 - speaker recognition, 195–196
 - typing dynamics, 198
 - ultrasonic/sonar biometrics, 187–188
- terminology, biometric, 21–22
- testing a biometric system. *See also*
 - implementing a biometric system; testing on-site
 - cost of, 134
 - industry groups' test data, 135–136
 - installing a testing system, 136–139
 - obtaining mature data, 134–135
 - overview, 17–18
- testing on-site. *See also* testing a biometric system; vendor/manufacturer
 - contacting manufacturer's customers, 135
 - industry data on, 135–136
 - installations for, 136–139
 - obtaining data on already-installed systems, 134–135
- theft prevention, 180, 251–252
- thermoelectric scanners, 65
- thermographic facial images
 - comparisons, 100, 256–257
 - defined, 272
 - future technologies, 193–194
 - overview, 99–100
- Third Factor Biometric Authentication News, 223
- threats. *See also* attacks; securing biometric systems; vulnerabilities
 - defined, 164, 274
 - manmade threats, 166
 - natural threats, 165–166
 - overview, 163–164
- 3D fingerprint image, 72–73
- 3D signature, 85–86
- timecard
 - biometric, 212–213
 - buddy punching, 250
- tools used in biometrics. *See also* scanners/readers
 - biometric flash drives, portable hard drives, 213–214
 - biometric timecard system, 212–213
 - business knowledge, 215–216
 - cardio-signature reader, 211
 - contactless palm-vein imager, 210
 - credit-card fingerprint scanner, 209–210
 - diplomacy skills, 215
 - laptop facial recognition, 212
 - mouse-embedded palm-vein scanner, 71, 210–211
 - survey skills, 214
- tracking individuals' activities, 57–58
- training
 - cost considerations, 126
 - defined, 274
 - for testing staff, 137–138
 - users, 17, 137–138, 152–153
 - translating voice into text, 103
- Transportation Worker Identification Credential (TWIC), 49, 275
- Triple A (AAA), 27, 66, 125–126, 269
- TWIC (Transportation Worker Identification Credential), 49, 275
- twins, identical
 - biometric tests using, 104
 - DNA of, 107
- 2D (two-dimensional) signature, 83
- two-factor authentication. *See* multifactor authentication

types of biometrics. *See also* comparing
 biometric solutions
 behavioral, 12–13, 200–201
 physical properties biometrics, 201–205
 physiological, 11–12
typing dynamics
 biometric basis for, 112
 comparisons, 117, 256–257
 described, 13, 111, 275
 future technologies, 198
 practical considerations, 112–113
 uses for, 113–114

• U •

ultrasonic/sonar biometrics,
 biometric basis for, 72
 comparisons, 73
 defined, 274, 275
 fingerprints, 65
 future technologies, 187–188
 overview, 71–72
 practical considerations, 72–73
 uses for, 73
Uncertainty Principle, Heisenberg's, 86–87
uniqueness, 14, 275
United Arab Emirates (UAE), 45, 94
United States. *See also* U.S. federal and state laws
 Department of Justice, 37, 220
 ports of entry, 47–49
 use of iris-recognition technology, 94
United States Visitor and Immigrant Status Indicator Technology (US-VISIT), 48, 56, 275
universality, 14, 275
updating the data, 14, 158, 159
upgrades, hardware, 161
U.S. Department of Justice, 37, 220
U.S. federal and state laws. *See also* legal issues
 data breach disclosure laws, 52–54
 Electronic Patient Health Information (EPHI), 54, 271
 overview, 46–47
users
 accepting biometric technology, 15
 behavior changes required of, 144–145
 with disabilities, 221–222
 enrollment, 13, 138

 health issues, 157–158
 helpdesk for, 155–156, 250
 information published for, 156–157
 locked out, 155–156
 needed for biometrics system, 132
 needs of, 24–25, 122
 privacy concerns, 127–128, 226–227
 problems with, 153
 safety of, 261
 sharing/stealing credentials, 10, 170
 as stakeholders, 129–130
 surveying, 214, 227
 training/educating, 17, 137–138, 152–153
 workloads, reducing, 250
US-VISIT (United States Visitor and Immigrant Status Indicator Technology), 48, 56, 275

• V •

vendor/manufacture. *See also* on-site testing; selecting a biometric system
 choosing, 139–140
 determining biometric requirements and, 131
 following up with, 140
 on-site testing through, 134–139
 reference contacts for, 133–134
 stability and support potential of, 139
 Web site resource, 222
video surveillance, 193, 266
virus biometrics, 203–204
voice. *See also* speaker recognition
 biometrics; speech
 range and harmonics of, 105
 recognition, 13, 27, 102, 275
 recording to use as fake credentials, 172
 translating into text, 103
vulnerabilities. *See also* attacks; securing biometric systems; threats
 database, 168
 defined, 164, 275
 identifying, 163–165
 matching flaws, 170
 operating-system, 167
 overview, 164–165, 166
 physical, 167
 replay, 170
 re-registration flaws, 170
 software, 168–169

• W •

walking, 13, 109. *See also* gait-recognition biometrics

Walt Disney World, 10

Web sites

- author's, 5
- Biometrics Catalog, 223–224
- Central Intelligence Agency (CIA), 41
- Electronic Frontier Foundation (EFF), 218–219
- European Union (EU), 55
- findBIOMETRICS, 222
- fingerprint misappropriation, 64
- International Center for Disability Resources on the Internet (ICDRI), 221–222

John Daugman, 224

National Biometric Security Project (NBSF), 135–136, 219

National Geographic, 217–218

security information, 183–184

Third Factor Biometric Authentication News, 223

U.S. Department of Justice, 37, 220

workloads, reducing, 250

• Y •

Young Frankenstein (film), 148