

Index

A

Access, 129, 181
 Account alerts, 148–149
 Accumulating data security, 162–164,
 167–170
 home protection during traveling,
 206–207
 Adapting, 165–170
 Alghamdi, Hamza, 110
 Alliance for Secure Business Information,
 71–72
 Almihdhar, Khalid, 110
 American Airlines Flight 77, 110
 AnnualCreditReport.com, 143, 144
 Antispyware, 79, 80
 Antivirus, 79, 80
 Apathy, 5–8, 62
 Arrogance, 62
The Art of Deception (Mittnick and Simon),
 118, 127, 131
The Art of War (Sun Tzu), 36
 ATMs, 25, 52–53
 Attorney, hiring, 220
 Authority bias, 117
 Automatic operating system updates, 81
 Auto-pay, 90
 AutoSafe, 60

B

Backing up data, 81
 Bank deposit slips, 52–53
 Banking during travel, 209–210

Benefits phase of interrogation, 133–134,
 136
 Bill payment:
 computer, 89–91
 traveling, during, 206
 Brain, engaging, 35–41
 enemy, knowing, 36–37
 mind-sets of spy, 37–40
 spy, thinking like, 35–36
 Brains. *See also* Brain, engaging
 as sources of identity, 22
 Bribe bias, 116
 “Business Case for Data Protection,”
 11
 Businesses, sources of identity, 22
 Business relevance:
 defining problem, 30–32
 destroying data, 71–72
 documentation, locking, 105–106
 interrogating enemy, 136–138
 laptop, protecting, 202
 monitoring signs, 152–153
 motivation, 10–12
 online identity, defending, 188–193
 recovering identity, 220–221
 risk, evaluating, 122–124
 securing systems, 92–93
 source of information, eliminating,
 61–63
 targeting enemy, 171–173
 traveling (business trips and vacations),
 211

234 Index

- C
- Car as source of information, 60
 - Cash, paying with, 54
 - CDs, destroying, 69–70
 - Cell phones:
 - cloning, 25
 - protecting, 225
 - as source of information, 59
 - travel, during, 208
 - Charm, 118
 - Checklists:
 - destroying data, 70
 - documentation, locking, 104–105
 - interrogating enemy, 136
 - laptop, protecting, 200–201
 - monitoring signs, 152
 - online identity, defending, 187–188
 - recovering identity, 213–220
 - risk, evaluating, 122
 - securing systems, 91
 - source of information, eliminating, 61
 - targeting enemy, 167–170
 - traveling (business trips and vacations), 210
 - Checks:
 - fraud, 51–52
 - traveling, during, 205
 - Check verification services, 217
 - freezing credit, 217–218
 - Chertoff, Michael, 43
 - Children, protecting, 88
 - Classification of documents, 105–106
 - Classification scheme and targeting enemy, 172
 - Clausewitz, Carl von, 155
 - C-level executives, Ponemon Institute Study, 11–12
 - Client files during travel, 204–205, 208
 - “Cloud computing,” 88, 188–193
 - Cluley, Graham, 176
 - Company data during travel, 205
 - Computer:
 - antispyware, 79, 80
 - antivirus, 79, 80
 - automatic operating system updates, 81
 - backing up data, 81
 - bill payment, 89–91
 - children, protecting, 88
 - “cloud computing,” 88, 188–193
 - electronic funds transfer, 90
 - encrypting hard drive, 83
 - encrypting wireless connections, 81–83
 - firewalls, 80
 - hacking, 25
 - laptop, protecting, protecting, seeie Laptop
 - mobile computing, 224–226
 - paper statements, replacement of, 89
 - partner, protecting, 88
 - passwords, protecting, 83–86
 - phishing scams, recognizing, 86–87
 - pop-up blockers, 81
 - protecting identity, prioritizing, 224–225
 - securing, 76–79
 - security software, 79
 - sources of identity, 21
 - spouse, protecting, 88
 - use of to prevent identity theft, 88–91
 - Contests, 57–58
 - Control:
 - access, 129
 - interrogating enemy, 128–130, 136
 - mobile data device responsibilities and best practices, 197, 198
 - need-to-know basis, 129–130, 136
 - Cookie (Google), 185
 - Cost per compromised record of breach, 33
 - Court record monitoring, 147

- Credit cards:
 - canceling, 145
 - destroying, 66–67
 - in mail, 104
 - offers of, 55–56
 - receipts, 52
 - rotating, 53–54
 - skimming, 120–121
 - traveling, during, 205
- Credit file:
 - fraud alert, 215
- Credit freeze, 48–50, 165, 217–218
 - protecting identity, prioritizing, 223
- Credit, generally
 - protecting identity, prioritizing, 223
- Credit offers, 55
- Credit report, 48–50. *See also* Credit report, monitoring
 - checking, 215
- Credit report, monitoring, 143–148, 223
 - identity monitoring services, 146–148, 223
 - what to monitor, 144–146
- Critical data, average rank of, 31
- Cross-site scripting, 25
- Culture of Privacy:
 - building, 11–13, 157–162
 - empowerment of team, 12–13
 - failure, building from, 157–162
 - interrogating enemy, 136–137
 - and interrogation, 127
 - leading by example, 13
 - and motivation, 12
- Curiosity, 127
- D**
- Data breach, 4, 5. *See also* Identity theft
 - cost of average, 7, 8
 - cost per compromised record of breach, 33
 - described, 25
 - Fifth Annual U.S. Cost of Data Breach Study, 34, 94
 - pre-record cost of, 76
 - prevention of, 10
 - primary sources of, 195
 - social networking, 180
 - third-party error, 130
 - use of term, 30
- Data, destroying. *See* Destroying data
- Data identity, 16
- Data warehouses, 22
- “Dead drop,” 102
- Debit cards, 52
 - traveling, during, 205
- Defining problem, 16–34
 - business relevance, 30–32
 - common methods of theft, defining, 27–28
 - failure to define, 32–34
 - how identities are stolen, 23–24
 - identity, defining, 16–19
 - sources of identity, 19–22
 - types of identity theft, 28–29
- Definition and targeting enemy, 172
- Destroying data, 37–38, 64–72
 - business relevance, 71–72
 - CDs, 69–70
 - checklist, 70
 - credit cards, 66–67
 - digital information, 69–70
 - disks, 69–70
 - documents, 66–67
 - failure, building culture of privacy from, 159
 - files, 66–67
 - laptop, protecting, 200
 - physical information, 66–69

236 Index

- Detection:
 - fraud, 141, 149
 - identity theft, 212–213
 - Digital assets, securing, 38
 - Digital information, destroying, 69–70
 - Directories, 57
 - Discounts, 57–58
 - Disks, destroying, 69–70
 - Distraction, 110–112
 - Distress bias, 117
 - Documentation. *See also* Documentation, locking; Physical documents
 - destroying, 66–67
 - Documentation, locking, 94–106
 - action item checklist, 104–105
 - business relevance, 105–106
 - classification of documents, 105–106
 - essential documents, how to lock, 98–100
 - failure, building culture of privacy from, 161
 - fire, documents to protect against, 99
 - flood, documents to protect against, 99
 - inside jobs, 94–95
 - mail, securing, 102–104
 - physical documents, 100–102
 - safe houses, 96–97
 - safe rooms, 97–98, 226
 - storage, 98
 - theft, documents to protect against, 99, 100
 - Dollar value gained by thieves, 27–28
 - Do Not Call Registry, 224
 - Do Not Mail list, 224
 - Dossier, creation of, 142–143
 - Driver's license, 30, 53, 219
 - Drop and switch, 45–47
 - Dumpster diving, 25, 64–65
-
- E
 - Education:
 - failure, building culture of privacy from, 162
 - and targeting enemy, 172
 - Electronic funds transfer, 90
 - Eliminating the source. *See* Source of information, eliminating
 - E-mail:
 - phishing, 121–122
 - protection of address, 185
 - Emotional biases, 115–118
 - Empowerment of team, 12–13
 - Encryption:
 - hard drive, 83
 - and targeting enemy, 172
 - wireless connections, 81–83
 - Enemies of privacy, 5–8
 - interrogating, 39
 - knowing, 36–37
 - Equifax, 49, 143, 144
 - address, 50
 - Essential documents, how to lock, 98–100
 - Evaluating risk. *See* Risk, evaluating
 - Evil twinning, 25
 - Excess credit, 52
 - Experian, 49, 143, 144
 - address, 50
 - Extended Validation SSI, 87
-
- F
 - Facebook. *See also* Social networking
 - development stage, 175
 - “5 Facebook Schemes That Threaten Your Privacy” (Cluley and Raphael), 176
 - and identity theft, 73–75
 - privacy settings, 182
 - protecting identity, 226

- quizzes, 179, 183
- safety, steps to, 181–187
- surveys, 183
- FACTA. *See* Fair & Accurate Credit Transaction Act (FACTA)
- Failure, building culture of privacy from, 157–162
 - defining problem, 158
 - destroying data, 159
 - documentation, locking, 161
 - improvement, ongoing, 162
 - monitoring, 162
 - and motivation, 3–5, 158
 - securing systems, 159–160
 - social engineering training, 161–162
- Fair & Accurate Credit Transaction Act (FACTA), 71, 102
- False communities, social networking, 180
- Family. *See* Friends and family
- Fear bias, 117
- Federal Trade Commission (FTC), 140
 - identity theft victim's report with, 218
 - Red Flags Rules, 71
- Fifth Annual U.S. Cost of Data Breach Study, 34, 94
- Files, destroying, 66–67
- Financial institutions, opt-out information, 56
- Financial transactions, monitoring, 148–150
- Fire, documents to protect against, 99
- Firewalls, 80
- "5 Facebook Schemes That Threaten Your Privacy" (Cluley and Raphael), 176
- Flattery bias, 117, 118
- Flood, documents to protect against, 99
- Franklin, Benjamin, 163, 165
- Fraud:
 - detection, 141, 149
 - friendly fraud, 25
 - recovery costs, 149
 - self-detection, 141, 146
 - "Fraud alert," 49–50, 223
- Freezing credit. *See* Credit freeze
- Friends and family:
 - Facebook, 226
 - and identity theft, 23, 25, 139–140
- FTC. *See* Federal Trade Commission (FTC)
- G**
- Gmail, 76, 77
- Goldsmith, Marshall, 6, 61–62
- Google, 185–187
 - cookie, 185
 - gmail, 76, 77
 - Google Docs, 187
 - Google Earth, 186
 - Google Mail, 186
 - Google Maps, 186
 - toolbar, 185–186
- Government cards, 53
- Greed, 62–63
- H**
- Hacking, computers, 25
- Heartland Payment Systems, 4, 7
- Hersh, Seymour, 110
- Hijacked profiles, social networking, 179
- "Hogwash" reflex, 114–119, 136
- Home, production during traveling, 206–207
- Home sources of identity, 20–21
- Hypocrisy, 63
- I**
- Identity. *See also* Identity theft
 - attributes of, 17–19
 - data identity, 16

238 Index

- Identity. *See also* Identity theft (*Continued*)
 defining, 16–19
 sources of, common, 19–22
- Identity creep, 163
- Identity monitoring services, 146–148, 223
- Identity theft. *See also* Data breach
 character/criminal, 29
 common methods of theft, defining, 24–28
 computer, use of to prevent, 88–91
 driver's license, 30
 and Facebook, 73–75
 financial, 28–29
 friends and family, 23, 139–140
 how identities are stolen, 23–24
 medical, 29–30
 monitoring, signing up for, 216
 profitability of identity to thief, 24
 restoration, 147
 Social Security number, 29
 and technology, 23
 types of, 28–30
 use of term, 31
 warning signs, 212–213
- Identity theft insurance, 147
- Identity theft victim's report with FTC, 218
- ID theft affidavit, 215
- Ignorance, 5–8, 62
- Impersonation, 178–179
- Improvement, ongoing, 162
- Inaction, 5–8
 example of, 8–10
- Information commerce, 54–58
- Information Week*, 178
- In public, sources of identity, 22
- Inside jobs, 94–95
- Insider theft, 172
- Internet:
 surveillance, 147
 travel, during, 208
- Interrogating enemy, 39, 125–138
 action item checklist, 136
 benefits phase, 133–134, 136
 business relevance, 136–138
 control phase, 128–130, 136
 justify phase, 130–131, 136
 phases of, 128–134
 risk scenarios, 134–135
 techniques, 132–133
- J**
- Javelin Strategy & Research. *See* 2009 Identity Fraud Report
- Junk mail, 54–58
- Justify phase of interrogating enemy, 130–131, 136
- K**
- Kaste, Martin, 181
- Keyhole, 186
- Keylogging, 26
- Koobface virus, 179
- L**
- Laptop, protecting, 41, 88, 194–202
 action item checklist, 200–201
 business relevance, 202
 destroying data, 200
 locking up, 198–199
 monitoring, 199
 and traveling, 204, 207–208
- Leading by example, 13
- Lock boxes, 103
- Locking documents, 38–39
- Logs, 151–152

M

Mail:

- securing, 102–104, 226
- as source of information, 58–59

Mailed statements, 150

Malicious widgets, 179–180

Malvertisements, 180

Malware, 179

- social networking, 79

Media Access Control (MAC), 82–83

Medical cards, 53

Medical identity theft, 29–30

Midnight mailing, 26

Military ID cards, 53

Mind-sets of spy, 37–40

- destroying, 67–68
- and destroying data, 64–72
- eliminating, 47–48
- and evaluating risk, 107–124
- interrogating enemy, 125–138
- and locking documentation, 94–106
- monitoring signs, 139–153
- online identity, defending, 174–176
- and securing systems, 73–93

Mitnick, Kevin, 118, 127, 131

Mobile data device responsibilities and best practices. *See also* Laptop, protecting and targeting enemy, 172, 196–200

Monitoring signs, 39–40, 139–153

- action item checklist, 152
- business relevance, 152–153
- credit report, monitoring, 143–148
- dossier, creation of, 142–143
- failure, building culture of privacy from, 162
- financial transactions, monitoring, 148–150
- logs, 151–152
- photocopies, 151–152, 206

Social Security statements, monitoring, 151

tools to implement, 153

Motivation, 3–15

- business relevance, 10–12
- and failure, 3–5, 158
- and inaction, 5–10
- and targeting enemy, 172

MySpace, 184

N

Name-dropping, 119

National Do Not Call Registry, 56

Need-to-know basis, 129–130

New Yorker, 110

Nonconfrontation bias, 117–118

Noncredit loan monitoring, 147

O

Observation, 109, 111, 119–122

Office, production during traveling, 207

Online identity, defending, 41, 174–193.

- See also* E-mail; Facebook; Google;
- Social networking

action item checklist, 187–188

business relevance, 188–193

mind-set, defending, 174–176

prioritizing, 226–227

sources of identity, 21–22

Online receipt of statements, 58

Online statements, 149–150

On person, sources of identity, 19–20

Opt-out addresses, 55

Opt-out information, 56

Outside Lies Magic (Stilgoe), 112

Overnight delivery services, 104

240 Index

- P**
- Paper statements, replacement of, 89
 - Paralysis, 63
 - Passport Office, contacting, 219
 - Passports, 208
 - Passwords:
 - cell phones, 225
 - computer, 83–86
 - hacking, 178
 - as source of information, 59
 - in wallets and purses, 52
 - Pentagon, 11
 - terrorist attack, 110
 - Pharming, 26
 - Phishing, 26
 - e-mail scams, 121–122
 - recognizing scams, 86–87
 - social networking, 180
 - Phone service, securing, 219
 - Photocopies, 53, 151–152, 206
 - Photo ID required, 53, 224
 - Physical documents, 100–102. *See also*
 - Documentation
 - protecting identity, prioritizing, 226
 - Picasso, Pablo, 65
 - PIN numbers, 52
 - P.O. boxes, 103
 - Police reports, 216
 - Ponemon Institute:
 - documentation, locking, 105
 - Fifth Annual U.S. Cost of Data Breach Study, 34, 94
 - Fourth Annual U.S. Cost of Data Breach Study, 130, 171
 - interrogating enemy, 137
 - Ounce Labs Study, 11
 - “Ponemon Business Case for Data Protection Report,” 173
 - pre-record cost of data breach, 76
 - “Security of Paper Documents in the Workplace,” 32
 - Poor Richard’s Almanac*, 163
 - Pop-up blockers, 81
 - Postal inspector, notification of mail theft, 219
 - Pretexting, 26
 - Prevention, 36
 - Principles of War* (von Clausewitz), 155
 - Prioritizing, 164–165, 167–170. *See also*
 - Protecting identity, prioritizing
 - “The Privacy Jungle. On the Market for Data Protection in Social Networks,” 182
 - Privacy reflex, 113–110
 - Privacy Rights Clearinghouse, 195
 - Proceedings of the National Academy of Sciences*, 177–178
 - Procrastination, 63
 - Professional, hiring, 77–78
 - Profile building, social networking, 177
 - Profitability of identity to thief, 24
 - Protecting identity, prioritizing, 41, 222–228
 - account alerts, 223
 - computers, 224–225
 - credit, 223
 - credit freeze, 223
 - identity monitoring services, 146–148, 223
 - mail, securing, 226
 - mobile computing, 224–226
 - online, 226–227
 - photo ID required, 53, 224
 - physical documents, 226
 - social engineering, 227–228
 - Social Security statements, monitoring, 228
 - travel, 227
 - wallets, 223–224

- Public record monitoring, 147
- Purses. *See* Wallets and purses
- Q**
- Quizzes, social network sites, 179
- R**
- Raphael, J.R., 176
- Reagan, Ronald, 131
- Recovering identity, 41, 212–221
 - action items checklist, 213–220
 - attorney, hiring, 220
 - business relevance, 220–221
 - check verification services, 217
 - cost of by source of theft, 28
 - credit file, fraud alert, 215
 - creditors, alerting, 214
 - deactivating accounts, 213–214
 - driver's license, safeguarding, 219
 - identity theft monitoring, signing up for,
 - 216
 - identity theft victim's report with, FTC,
 - 218
 - ID theft affidavit, 215
 - Passport Office, contacting, 219
 - phone service, securing, 219
 - police report, filing, 216
 - postal inspector, notification, 219
 - Social Security Administration,
 - contacting, 219
 - statements, monitoring, 217
 - Theft Resource Center, 220
 - warning signs of identity theft, 212–213
- Red-flagging, 26, 71
- Requests for identity, 113–114
- Risk, evaluating, 39, 107–124
 - action item checklist, 122
 - business relevance, 122–124
 - examples of, 120–121
 - mind-set, evaluating, 108–109
 - and observation, 109, 111, 119–122
 - privacy reflex, 113–110
 - requests for identity, 113–114
 - social engineering, 107–108, 110–112
- Risk scenarios, interrogating enemy, 134–135
- Roethke, Theodore, 111
- Rush bias, 116, 118
- S**
- Safe houses, 96–97
- Safe rooms, 97–98, 226
- Secret Crush widget, 180
- Securing systems, 38, 73–93
 - action item checklist, 91
 - business relevance, 92–93
 - computer, 76–79
 - failure, building culture of privacy from,
 - 159–160
 - professional, hiring, 77–78
- Security, 10–11
 - bias, 115–116
- Security freeze. *See* Credit freeze
- “Security of Paper Documents in the Workplace” (Ponemon Institute), 32
- Security software, 79
- Sensitive information, exposure, 166
- SentrySafe, 60
- September 11, 2001, 110–111
- Service Set Identifier (SSID), 82
- Sex offender reports, 147
- Shoulder surfing, 26, 120
- Shredding:
 - and convenience, 66
 - cross-cut confetti, 68
 - electronic, 69
 - purchase of shredders, 72
 - and targeting enemy, 172

242 Index

- Signature required, 53
- Simmel, George, 130
- Simon, William, 118, 127, 131
- Skimming, 27
 - ATM skimming, 25
- Slippery slope bias, 117
- SMiShing, 27
- Social engineering, 27
 - and authority, 118
 - authority bias, 117
 - bribe bias, 116
 - charm, 118
 - corporate, 125–127
 - and distraction, 110–112
 - distress bias, 117
 - emotional biases, 115–118
 - failure, building culture of privacy from, 161–162
 - fear bias, 117
 - flattery bias, 117, 118
 - “Hogwash” reflex, 114–119, 136
 - name-dropping, 119
 - nonconfrontation bias, 117–118
 - protecting identity, prioritizing, 227–228
 - requests for identity, 113–114
 - rush bias, 116, 118
 - security bias, 115–116
 - slippery slope bias, 117
 - social networking, 178
 - trust bias, 115
- Social networking. *See also* Facebook
 - data breach, 180
 - development stage, 175
 - false communities, 180
 - hazards of, 176–181
 - hijacked profiles, 179
 - impersonation, 178–179
 - malicious widgets, 179–180
 - malvertisements, 180
 - malware, 79, 179
 - password hacking, 178
 - phishing, 180
 - profile building, 177
 - public nature of, 183
 - quizzes, misleading, 179
 - and skepticism, 184–185
 - social engineering, 178
 - Social Security number capture, 177–178
 - and trust, 176
 - Social Security Administration, contacting, 219
 - Social Security cards, 51
 - traveling, during, 205–206
 - Social Security numbers:
 - capture, social networking, 177–178
 - and identity, 16
 - identity theft, 29
 - vulnerability, 6
 - Social Security statements, monitoring, 151, 228
 - Source of information, eliminating, 37, 45–63
 - action item checklist, 61
 - business relevance, 61–63
 - car, 60
 - cell phones, 59
 - credit report, 48–50
 - drop and switch, 45–47
 - information commerce, 54–58
 - junk mail, 54–58
 - mail, 58–59
 - mind-set of spies, 47–48
 - passwords, 59
 - spam, 60
 - and targeting enemy, 172–173
 - telemarketing, 54–58
 - wallets and purses, 50–54
 - website data leakage, 59–60

- Spam as source of information, 60
- Spinney, Mike, 137–138
- Spouse, protecting, 88
- Spy:
 - mind-sets of, 37–40
 - thinking like, 35–36, 43
- Squares test, 111–112
- Stealing, 26
- Steinmetz, Charles P., 127
- Stilgoe, John, 112
- Storage, documents, 98
- Student ID cards, 53
- Sun Tzu, 36
- Surveys, 58
 - Facebook, 183
- T**
- Targeting enemy, 40–41
 - accumulating data security, 162–164, 167–170
 - action items, 167–170
 - adapting, 165–167, 167–170
 - business relevance, 171–173
 - classification scheme, 172
 - and education, 172
 - encryption, 172
 - failure, building culture of privacy from, 157–162
 - generally, 155
 - insider theft, 172
 - laptop, protecting, 41, 88, 194–202
 - mobile data device responsibilities and
 - best practices, 41, 172, 196–200
 - and motivation, 172
 - online identity, defending, 41, 174–193
 - principles, 162–170
 - prioritizing, 164–165, 167–170
 - protecting identity, prioritizing, 41, 222–228
 - recovering identity, 41, 212–221
 - shredding, 172
 - source of information, eliminating, 172–173
 - strategies, 40–41, 157–173
 - traveling (business trips and vacations), 41, 203–211
- Technology and identity theft, 23
- Telemarketing, 54–58
- Theft, documents to protect against, 99, 100
- Theft Resource Center, 220
- 3-in-1 credit monitoring, 147
- TJX, 4, 7
- Toolbar (Google), 185
- TransUnion, 49, 143, 144
 - address, 50
- Traveling (business trips and vacations), 41, 203–211
 - action item checklist, 210
 - banking, 209–210
 - belongings, carrying, 208–209
 - bill payment, 206
 - business relevance, 211
 - cell phones, 208
 - checks and checkbooks, 205
 - client files, 204–205, 208
 - company data, 205
 - credit cards, 205
 - debit cards, 205
 - home, production during, 206–207
 - identification, 205–206, 208
 - Internet, public access, 206
 - laptops, 204, 207–208
 - before leaving home, 204–207
 - office, production during, 207
 - passports, 208
 - protecting identity, prioritizing, 227
 - Social Security cards, 205–206

244 Index

- Traveling (business trips and vacations)
(*Continued*)
during travel, 207–208
traveling light, 204–206
- Trojan horse, 27
- Trust:
bias, 115
social networking, 176
- 2009 Identity Fraud Report:
destroying data, 68
fraud, detection, 141, 212
identity, defined, 16–17
mail, protecting, 104
medical identity theft, 30
monitoring signs, 152
on paper trails, 59
recovering identity, 212,
214
safe houses, 97
sources of identity, 19
- U
- United Flight 175, 110
- U.S. Department of Defense, 11
- U.S. Department of Veterans Affairs,
4
- U.S. Postal Inspection Service, 103
- V
- Verify:
mobile data device responsibilities and
best practices, 197
- Vishing, 27
- W
- Wallets and purses:
protecting identity, prioritizing, 223–224
as source of information, 50–54
- Wardriving, 27
- Warning signs of identity theft, 212–213
- Warranty cards, 58
- Website data leakage as source of
information, 59–60
- WEP (Wired Equivalence Privacy), 82
- What Got You Here Won't Get You There*
(Goldsmith), 6, 61–62
- White pages, 57
- Wi-Fi Protected Access, 82
- Woods, James, 110–111
- World Privacy Forum, 191–193
- World Trade Center attacks, 110–111
- WPA2, 82
- Z
- Zabasearch, 57