

Index

- Abdulmutallab, Umar Farouk, 143, 211–212, 305n87
- Abu Ghraib, 204
- Abu-Jihaad, Hassan, 109
- Advanced Encryption Standard (AES), 45, 46–47, 231, 272n36
- “Adventure of the Dancing Men, The” (Doyle), 43
- Adus, Hamdi Isaac, 100
- Afghanistan, 88, 94, 135, 223, 228
- Air gapped systems, 143, 180–181
- Alcatel-Lucent, 173
- Alien and Sedition Acts, 256
- Al-Haramain, 92, 94
- Al-Harhi, Qaed Senyan, 107
- Al-Qaeda, 2, 94, 210, 284n117
- Bin Laden and, 139
- Brooklyn Bridge and, 88
- effectiveness of surveillance and, 107–112
- global cooperation and, 208
- phone cards and, 98
- Sears Tower and, 108
- water supply and, 161
- Zazi and, 111
- Amazon, 42, 49
- ecommerce and, 45
- Elastic Compute Cloud (EC2) and, 126
- evolving communication technologies and, 123
- patents and, 31
- open access to, 59, 239–240
- American Civil Liberties Union (ACLU), 92, 176, 288n156
- American Indians, 45
- Ames, Aldrich, 98, 162
- Amnesty International, 176
- Anderson, Ross, 242
- Anonymization, 139–141, 191, 222, 321n64. *See also* Attribution
- Anthrax attacks, 222
- Anti-Vietnam War protests, 68, 73, 175
- AOL, 22, 32
- Apple
- iPhones, 4, 6–7, 33, 99, 127, 134, 230
- iPods, 154, 155–157, 173
- Application layer, 25
- Area codes, 14, 16, 194
- ARPANET, 19–21, 27, 37–40, 263n40
- Arthashastra* (ancient Indian writing), 43
- Ashcroft, John, 85, 91
- Asian Development Bank, 167
- AT&T, 2, 4, 240, 258n8
- Alcatel-Lucent and, 316n180
- Baran and, 18–19
- breakup of, 81
- Carterfone and, 5–6
- Clipper and, 114–115, 196
- communication during crises and, 230
- communication network architectures and, 18, 266n71

- AT&T (cont.)
 cryptography and, 44, 59
 deep packet inspection and, 132
 denial of service and, 181–182
 Einstein projects and, 121, 219
 evolving communication technologies and, 132, 303n56
Hepting case and, 92–93
 legal issues and, 81, 88–89, 92–93, 121, 279n45, 288n159
 Klein and, 176–177
 monopoly of, 5
 Narus machines and, 176
 network convergence and, 181–182
 secret room of, 176–177
 security risks and, 176–177, 181, 187, 196–199, 317nn10,11, 319n35
 traffic analysis and, 176–177
 TSD 3600 and, 114–115
 warrantless wiretaps and, 88, 92–93
 wireless systems crash, 103
- Athens Affair, 3–4, 177, 187, 234–235, 240–241
- ATMs (Automatic Teller Machines), 160, 242, 273n59
- Atomic bomb, 8
- Attacks, 8–9, 95, 153, 208, 236
 Aurora, 159
 blue box, 39–40, 196, 270n12
 botnets and, 53, 145–146, 234, 305n2, 333n7
 China and, 166–171
 critical infrastructure risks, 157–161
 custom, 234
 cybersecurity and, 234 (*see also* Cybersecurity)
 DDoS, 53–55, 58, 120, 146, 161, 235
 ease of, 255
 Heartland Payment Services and, 160
 hosts and, 53–55, 146
 infrastructure risks and, 157, 234–235
 insider, 162–165
 malware and, 53–55, 120–122, 145, 181–182, 219–221, 234, 240, 312n111
 National Infrastructure Protection Plan and, 157
 by nation-states, 165–171
 nuclear power plants and, 159
 phishing, 52, 58
 progress in protection from, 172–173
 proliferation of, 48
 RBS WorldPay and, 160
 rootkits and, 146
 routers and, 48
 script kiddies and, 145
 sniff packets and, 53, 85, 160, 178–179, 199
 Trojan horses and, 54, 94, 146, 166–167, 170
 Tutelage and, 219
- Attribution, 35, 57–59
- Aurora, 159
- Australia, 113, 141, 152, 159, 167, 235
- Authentication, 34, 157–158, 172
 difficulty of, 46–47, 53, 57–63, 276n86
 effectiveness of, 113–116
 firewalls and, 55, 131, 159, 233–234, 238, 240, 265n59, 273n44
 IPsec and, 62–63
 lack of in TCP/IP, 40–41
 right policy for, 237, 249–250
 root nameservers and, 49, 51, 53, 61–62
 security risks and, 180–181, 185
 spoofing and, 52–55, 58, 60–61, 113, 187, 196
 trust anchor and, 61–62
- Authorization for Use of Military Force (AUMF), 93
- Availability, 38–42
- Backbone networks, 38, 324n114
- Baidu.com, 142

- Baker, James, 90, 92, 208
 Baker, Stewart, 121–122, 297n113
 Balkin, Jack, 288n157
Baltimore Sun, 119
 Baran, Paul, 17–19, 28, 37–38
 Barcodes, 127
 Bell, Alexander Graham, 7, 13, 19
 BellSouth, 88, 228
 Benetton, 154–155, 309n68
 Benkler, Yochai, 33
 Berners-Lee, Tim, 141
 Berson, Tom, 179
 Bhagwati, Jagdish, 213
 Bill of Rights, 1, 10, 67, 189–190.
 See also First Amendment; Fourth
 Amendment; Fifth Amendment;
 Tenth Amendment
 Bin Laden, Osama, 139
 Biotechnology, 150
 BITNET (Because It's There Net), 21
 BitTorrent, 34–35, 132
 Black-bag job, 71, 133
 BlackBerry, 7, 127, 133, 181–182
 Black Friday, 135
 Blaze, Matt, xv, 196, 199
 Blogger, 142
 Blogs, 31, 141–142, 267n85, 268n87
 Bloody Sunday, 206–207
 Bloomberg, Michael, 209, 226
 Blue box attacks, 39–40, 196, 270n12
 Bluetooth technology, 303n55
 Boeing, 149
 Bolt Beranak and Newman (BBN),
 19
 Botnets, 53, 145–146, 234, 305n2,
 333n7
 Brandeis, Louis, 10, 67, 260n43,
 312n115
Brazenburg v. Hayes, 204
 Bristol-Myers-Squibb, 150
 British Telecom, 131
 Brookson, Charles, 113
 Bugs, 9, 69, 70, 104, 106, 197, 249
 Bundesnachrichtendienst (BND), 94
 Bureau of Alcohol, Tobacco, Firearms
 and Explosives, 108
 Burgess, Guy, 163, 311n103
 Burma, 215
 Bush, George H.W., 81
 Bush, George W., xiii, 336n41
 Authorization for Use of Military
 Force (AUMF) and, 93
 effectiveness of wiretapping and, 97,
 108, 111, 120
 legal issues and, 88–95
 National Security Presidential
 Directive 54 and, 120
 policy risks and, 203–204, 207–208
 President's Surveillance Program (PSP)
 and, 88, 90–95, 112, 176, 200, 203,
 243, 252, 256, 286n137, 338n3
 rule of law and, 208
 security risks and, 176
 SWIFT database and, 111
 warrantless wiretaps and (*see*
 President's Surveillance Program)
 Business communications, 147–152
 Cables, 3, 270n17
 communication during crises and,
 227, 229
 communication network architectures
 and, 14, 22
 evolving communication technologies
 and, 123, 128, 131, 301n30
 fiber-optic, 22, 72, 87, 89, 123, 157,
 226–227, 306n18, 331n12
 transoceanic, 4, 88, 285n127
 wiretapping and, 72, 78, 80, 87,
 285n127
 Caching, 51–52, 63, 276n88, 331n12
 Caesar cipher, 43
 Call Content Channel (CCC), 29, 83
 Call Data Channel (CDC), 29, 83
 Call Detail Records (CDRs), 89, 200
 (*see also* Transactional information)

- CISPES investigations and, 176
 communities of interest and, 136
 deep packet inspection and, 130–133, 219–222
 effectiveness of wiretapping and, 99, 102
 excessive collection risks and, 192–195
 hot numbers and, 194
 right policy stance for, 240, 248
 rule of law and, 207–208
 sneak peeks and, 194
 Call forwarding, 29, 72, 81
 Cambridge Five, 162
 Cambridge University, 138
 Cameron, David, 206–207
 Campbell, Duncan, 152
 Campus networks, 38, 42, 239, 264n48
 Canada, 55, 113, 116, 121, 152, 161, 244
 Card, Andrew, 91
 Carnivore, 85, 187, 196, 243, 245
 Carter, Jimmy, 215
 Carterfone, 5–6, 258n20, 259n21
 Catholics, 206–207
 CBS, 34, 69
 Celanese, 150
 Cell phones, 1, 3–4, 7, 172
 annual U.S. usage of, 30
 call length and, 134
 communication network architecture and, 13, 26, 29–31, 265n52, 267n85
 denial of service and, 181–182
 design principles and, 42
 effectiveness of tapping, 98–103, 107, 113
 E911 and, 129
 evolving communication technologies and, 128–130, 134, 302n40
 functionality during crises and, 226–227
 Gamma Guppy intercepts and, 135
 GSM and, 113
 high-speed trains and, 265n52
 Home Location Register and, 26, 183
 improving security of, 178
 legal issues and, 64, 80–81, 84
 Mobile Switching Center (MSC) and, 129, 183, 248
 network convergence and, 180–182
 right policy stance for, 236, 248–249
 roaming and, 26–27, 182–187
 security risks of, 177–187, 199
 targeted advertising and, 103–104
 Visitor Location Register and, 26
 Censorship, 218
 Centers for Disease Control and Prevention (CDC), 125
 Central Intelligence Agency (CIA), 209, 260n40, 284n117
 Ames and, 162
 critical infrastructure risks and, 161
 deep packet inspection and, 221
 economic espionage and, 151–153
 effectiveness of wiretapping and, 98, 112
 evolving communication technologies and, 135, 141, 143
 identifying intruders and, 151–152, 161–163
 insider attacks and, 162–163
 Langley and, 143
 legal issues and, 75, 94–95
 NGOs and, 217
 traffic analysis and, 135
 Woolsey and, 152, 153
 Cerf, Vinton, 20, 23, 24, 37–39, 48
 Chabinsky, Steve, 172
Challenge of Crime in a Free Society, The (report), 73
Charles Katz v. United States, 11, 70
 Charter Communications, 131
 Chat rooms, 140
 Chaum, David, 139
 China, xi–xii, 6, 87, 235, 255, 297n113, 334n9
 cell phone use in, 29

- communication network architectures
and, 29–30, 266n70, 267n86
- communication networks role in
economic growth and, 213–214
- credit cards and, 172
- economic espionage and, 153
- evolving communication technologies
and, 133, 142
- Google and, 170
- Great Firewall of, 55
- hackers and, 166–169
- industrial espionage and, 168–169, 171
- intruder identification and, 150,
153–154, 166–173, 313n127,
314nn144,152
- limited freedoms in, 267n86
- People Liberation Army and, 235
- policy risks and, 213–214
- security risks and, 52, 55, 179, 197
- spying and, 166–171
- supply chain issues and, 197
- Taiwan and, 167–168
- texting and, 29–30
- Tibet and, 167–168
- Titan Rain and, 167, 170
- Tom-Skype and, 179
- U.K. Parliament and, 167
- U.S. military information and,
166–167
- Church Committee, 60, 69, 77, 175
- Cie. des Machines Bull, 149
- Cisco, 274n61, 316n176, 324n114
attacks on equipment of, 52
counterfeiting routers of, 6, 173
exploiting security risks of, 196, 235,
241, 243, 335n31, 337n57
- Citibank, 160
- City of Ontario, California et al.,
Petitioners v. Jeff Quon*, 121
- Civil rights, 97, 175
- Bloody Sunday and, 206
- European Convention on Human
Rights and, 203
- Europol and, 136–137
- legal issues and, 69, 73, 85
- Universal Declaration of Human
Rights and, 203
- Clark, David, xv, 238, 239
- Clark, Ramsey, 74–75
- Clinton, Bill, 32, 192
- Clinton, Hillary, 214, 218
- Clipper, 114–115, 195–196
- Closed-circuit TV (CCTV), xii
- Cloud computing, 53, 116, 125–127,
184, 228, 300n8, 301n27
- Code of Federal Regulations, 204–205
- Cohen, Danny, 27, 37
- Cohen, David, 210
- Cold War, 8, 17, 201, 213
- Ames and, 163–164
- attacks by nation-states and, 165–171
- Black Friday and, 135
- cryptography and, 113–114
- Hanssen and, 163, 165
- insider attacks and, 162
- Mutually Assured Destruction and,
215
- Philby and, 162–163
- RFID tags use during, 128
- Sputnik and, 19
- spying and, 146–149, 151
- traffic analysis and, 135
- Cole, David, 256
- Colombia, 110, 218
- Comcast, 131–132
- Comey, James, 91
- Committee in Solidarity with the
People of El Salvador (CISPES),
176
- Committee to Re-Elect the President,
76
- Communication networks
air-gapped, 143, 180–181
- area codes and, 14, 16, 194
- ARPANET and, 19–21, 27, 37–40,
263n40

- Communication networks (cont.)
- bandwidth and, 21, 24–25, 27, 124, 126, 131, 181–182, 189, 227, 264n51, 318n26
 - Baran and, 17–19, 28, 37–38
 - BITNET, 21
 - bursty traffic and, 17
 - Call Detail Records (CDRs) and, 89
 - copyright and, 218
 - centralized, 14–20, 27–28, 71, 178, 182, 184–186, 199, 226–227, 248
 - cloud computing and, 125–127
 - communication during crises and, 225–232
 - content and, 31–33
 - creating the Internet and, 17–21
 - CSNET, 21
 - cybersecurity and, 9, 95, 120, 208, 233–234, 242
 - data on voice, 28–30
 - Davies and, 17–19, 37–38
 - decentralized, 14, 18, 31, 33
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - Domain Name Servers (DNS) system and, 49–52, 60–63, 115–116, 142–143, 244, 263n31, 273n51, 276n88
 - economic growth and, 212–215
 - end-to-end encryption and, 47, 57, 59–60, 179, 195, 199, 222, 232, 246, 249, 336n47
 - friendship networks and, 138
 - fundamental design principles and, 19–20
 - grassroots communities and, 32
 - HEPNet, 21
 - international calls and, 4
 - interoperability issues and, 225–232
 - Land Mobile Radio (LMR) systems and, 229–231
 - layers of, 22–25
 - local exchange and, 14, 16, 78
 - local loop and, 71–72, 81–82
 - local networks and, 14, 16, 19, 21, 25–27, 51, 61–62, 78, 81, 116, 126, 128, 140, 172, 180, 183–187, 231
 - MFENet, 21
 - Mobile Switching Center (MSC) and, 129, 183, 248
 - modern, 78–85
 - Murphy's law and, 195–198
 - NAT boxes and, 127, 263n32, 300n11
 - network convergence and, 180–182
 - network effect and, 125, 241
 - network hosts and, 22, 32, 40, 48–49, 53–58, 132, 141, 146, 167, 169, 219, 234, 239, 249, 336n47
 - NSFNET, 21–22, 38, 42, 264n46
 - other IP-based, 21–22
 - partitioning of, 239–240
 - peering points and, 53, 89–90
 - peer-to-peer, 18, 28, 34–35, 56–57, 132, 183, 260n33, 265n59, 269n101, 300n18
 - protocol stack and, 23–25
 - railway system and, 13–14
 - redundancy and, 17–18, 21, 40, 270n13, 273n48
 - reliability and, 17–18, 21, 24, 38–40, 60, 233
 - repeaters and, 16, 230
 - root nameservers and, 49, 51, 53, 61–62
 - routing and, 4, 20–30, 48, 57, 59, 86, 139–140, 183, 185, 190, 234, 238–239, 262n15, 263nn31,34, 264n48, 275n77
 - Signaling System 6 and, 29, 39
 - Signaling System 7 and, 29, 79–80, 180–181, 265n62, 266n71
 - social, 56, 138, 191, 248
 - TCP/IP and, 20, 23–25, 37–42, 46, 53, 56, 132–133, 264nn50,51, 269n3
 - telephone, 13–17, 30–31
 - texting, 28–30
 - Tor, 139–140

- USENET, 21
 voice on data, 27–28
- Communications Assistance for Law Enforcement Act (CALEA), 2–3, 119, 292n31, 297n113
- Athens Affair and, 177
- Clipper and, 196
- compliance issues and, 240
- costs of, 249–250
- deep packet inspection (DPI) and, 219
- as Digital Telephony bill, 320n48
- excessive collection risks and, 190
- expansion of, 233, 248
- export control and, 119
- legal issues and, 82–85, 88, 284nn110,114
- limitation of, 246–248
- mobile security risks and, 186
- policy issues and, 203, 219, 223, 240, 245–250
- post-cut-through dialed digits and, 82, 84
- security risks and, 177, 186–190, 196, 200, 320n48
- threats to innovation and, 188–189
- VoIP and, 84–85
- wiretapping without, 248–250
- Communications interception. *See* Surveillance; Wiretaps
- Communications security, 47, 59–60.
See also Surveillance; Wiretaps
- cell phone design and, 113
- civil society and, 215–219
- Communications Assistance for Law Enforcement Act and, 246
- Deep Packet Inspection and, 221–222
- first responder systems and, 231–232
- government agencies and, 243–246
- Heartland Payment Services and, 160
- importance of to United States, 256
- Internet and, 39
- SCADA systems and, 158–159
- secure telephones, 114–115
- Software Defined Network paradigm for, 239–240
- wiretapping creating risks to, 175–202, 247–248 (*see also* Athens Affair)
- Communication technologies. *See also* Internet
- anonymization tools and, 139–141, 191, 222, 321n64
- automatic switching and, 4–5
- bandwidth and, 21, 24–27, 124, 126, 131, 181–182, 189, 227, 264n51, 318n26
- barcodes and, 127
- blogging and, 31, 141–142, 267n85, 268n87
- Bluetooth, 303n55
- botnets and, 53, 145–146, 234, 333n7
- caching and, 51–52, 63, 276n88, 331n12
- Carterfone and, 5–6, 258n20, 259n21
- cloud computing and, 53, 116, 125–127, 184, 228, 300n8, 301n27
- Cold War and, 8, 17, 113–114, 128, 135, 148, 151, 201, 213, 215
- compatibility of American and European systems and, 4–5
- connectivity and, 124
- cyberattacks and, 8–9, 95, 145–146, 153, 168, 171, 208, 235, 235–236, 333n7
- data parceling and, 124
- distributed computation and, 124–125
- fiber optics and, 22, 72, 87, 89, 123, 157, 226–227, 306n18, 331n12
- first revolution of, 123
- functioning during crises, 226–232
- future scenario for, 236–237
- GPS, 130
- importance of, xii
- Instant Messaging and, 24–25, 38, 140, 188, 227, 252, 298n116
- law enforcement issues and, 7–8 (*see also* Legal issues)

- Communication technologies. *See also*
 Internet (cont.)
 Martus and, 217–218
 mobility and, 8, 133–134, 186
 modern networks and, 78–85
 Moore's law and, 45
 online services and, 6–7
 operating systems and, 32–34, 52, 54, 56, 133, 146, 182, 202, 242, 274nn64,66, 335n24
 packet-switching and, 3, 8, 18–19, 38, 56, 178
 PANS (Pretty Advanced Network Services) and, 4
 pen registers and, 79–86, 89, 99–104, 133, 137, 187, 190, 194, 196, 219, 248, 285n120, 292n31, 337n63
 plethora of new, 248–249
 progress of, 123–143
 PSTN and, 4–6 (*see also* Public Switched Telephone Network (PTSN))
 radio and, 4–5, 7, 17, 26, 31 (*see also* Radio)
 repeaters and, 16, 230
 replication and, 123–124
 RFID tags and, 7, 127–128, 180–181, 259n29
 RSS feeds and, 31
 second revolution of, 123
 security risks of, 177–202
 signaling systems and, 4–5
 supercomputers and, 21, 38, 117, 124–125, 264n42
 surveillance and, 123, 130, 133, 142 (*see also* Surveillance)
 telegraph and, 1, 7, 13–14, 66, 123, 212–213
 telephone and, 128–130 (*see also* Telephones)
 television and, 31, 226
 texting and, 7, 29–30, 72, 121, 131–132, 179, 265n61, 266nn70,71, 319n39
 threats to innovation and, 188–189
 traffic analysis and, 133–138
 World Trade Center and, 226
 Communities of interest (COIs), 136
 Com nameserver, 49, 51, 61–62, 273n53
 Comprehensive National Cybersecurity Initiative (CNCI), 120
 Computer and Internet Protocol Address Verifier (CIPAV), 133, 245, 249
 Computer Security Act, 244
 Confidentiality, 2, 47
 communications and, 67, 173
 cryptography and, 60, 115
 VoIP and, 179
 Consensual overhear, 71, 106
 Coordinating Committee on Multilateral Export Controls (CoCOM), 113
 Corning, 149
 Council of Islamic-American Relations, 211
 Counterfeiting, 6, 160, 173, 273n59, 324n114
 Credit cards, 160, 172–173
 Crises
 first responders and, 226–232
 Information Assurance Directorate (IAD) and, 231–232
 interoperability and, 225–232
 Critical infrastructure risks, 157–161
 Cross, Tom, 196
 Crypto AG, 114
 Cryptography, 1, 98, 155, 196, 219, 280n58
 Advanced Encryption Standard (AES) and, 45, 46–47, 231, 272n36
 analyzing fielded communication products and, 113–117
 Black Friday and, 135
 brute-force decryption and, 114, 237, 249, 257n4, 271n27, 324n111
 Caesar cipher and, 43

- Clipper and, 114–115, 195–196
- CoCOM and, 113
- Cold War and, 113–114
- Comprehensive National Cybersecurity Initiative (CNCI) and, 120
- Computer Security Act and, 244
- Data Encryption Standard (DES) and, 44–45, 47, 114–115, 244, 257n4
- deep packet inspection and, 222
- digital signatures and, 46–47, 61
- Diffie and, 45–46
- DNSSEC and, 52, 60–62, 115–116, 142, 244
- dual-use status of, 114
- ECHELON and, 152
- end-to-end design and, 20, 31–32, 47, 57, 59–60, 132, 179, 195, 199, 222, 232, 236, 246, 249, 336n47 (*see also* Keys)
- Enigma machines and, 44, 271n24
- Escrowed Encryption Standard (EES) and, 114–115
- export control of, 116–119
- frequency analysis and, 44, 271n23
- governmental key storage and, 115
- GSM Algorithmic Experts Group and, 113
- Heartland Payment Services and, 160
- Hellman and, 45–46
- historical perspective on, 43–47
- inherent contradiction in, 43
- interoperability and, 231
- Kerckhoffs' Law and, 43
- Lotus Notes and, 116–117
- Mary Queen of Scots use of, 1
- Moore's law and, 45
- Navajo code talkers and, 45
- nonrepudiation and, 46, 60
- Office of Munitions Control and, 114
- one-time pad and, 44
- polyalphabetic substitution ciphers and, 44
- private-key cryptosystems (*see* public-key cryptosystems)
- public-key cryptosystems, 45–46
- radio's effect on use of, 43
- rotor machines and, 44, 271n23
- RSAREF and, 116
- Security and Freedom through Encryption Act and, 118
- signatures and, 46–47, 61–62, 281n65
- 64-bit, 116–117, 297n106
- Skipjack and, 114–115
- Skype and, 179
- strong, 2, 42, 46, 74, 114, 117–118, 257n4
- Suite B algorithms and, 47
- symmetric-key cryptosystems, 45 (*see also* Advanced Encryption Standard, Digital Encryption Standard)
- 32-bit, 116–117
- traffic analysis and, 134–139
- TSD3600 and, 114–115
- virtual private networks and, 46, 119, 179, 233, 336n47
- warfare and, 43, 43–44
- weak, 196, 280n58
- Crypto Wars, 2, 106, 113, 214
- CSNET, 21
- Cuba, 148, 258n3
- Cyberattack, 8–9, 145–146, 153, 168, 171, 235–236, 333n7
- Cyberexploitation, 146, 153, 165, 167, 169, 235
- Cybersecurity, 9, 95, 208, 242
- Computer and Internet Protocol Address Verifier (CIPAV) and, 133, 245, 249
- Computer Security Act and, 244
- deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
- destruction capabilities and, 235
- distinction from computer security, 233
- economic issues and, 241–243

- firewalls and, 55, 131, 159, 233–234, 238, 240, 265n59, 273n44
- future scenario for, 236–237
- hashing and, 47, 61, 237, 243–244, 272n38, 324n111, 337n57
- human values and, 238
- infrastructure risks and, 234–235
- limitation of CALEA and, 246–248
- malware and, 53–55, 120–122, 145, 181–182, 219–221, 234, 240, 312n11
- military and, 235–236, 255
- OpenFlow and, 238–239
- patches and, 35, 48, 56, 63, 166, 170, 227, 276n88
- right policy stance for, 243–246, 250–253
- right technical stance for, 237–241
- SAFECOM and, 244–245
- Software Designed Networks (SDNs) and, 239
- ubiquitous networks and, 233–234
- vendor responsibility and, 242
- Cylink, 114
- Czechoslovakia, 135

- Dagon, David, 52
- Dai Qingmin, 168
- Dalai Lama, 168
- Daniel, Hugh, 116
- Data Encryption Standard (DES), 44–45, 47, 114–115, 244, 257n4
- Data mining, 97, 136, 191, 252
- Datotek, 114–115
- Davies, Donald, 17–19, 37–38
- Davis-Besse nuclear plant, 159, 234
- DCS3000, 85, 187, 196, 243, 245
- Deciphering Information Society* (Dai), 168
- DEC VAX, 39
- Deep packet inspection (DPI), 130–133, 219–222, 234–235, 240–241
- Defense Advanced Research Projects Agency (DARPA), 19, 39, 47, 62, 123–124, 127, 141, 233, 238, 334n20
- Defense Information Systems Agency, 166
- Diffie, Whitfield, xv, 1, 45–47, 65, 106
- Digital fingerprints, 272n38
- Digital Telephony proposal, 81
- Direction Générale de la Sécurité Extérieure (DGSE), 148–149
- Distributed denial-of-service (DDoS) attacks, 53–55, 58, 120, 146, 161, 235
- DNS resolver, 51, 60–61
- DNSSEC (Domain Name System Security Extensions), 52, 60–62, 115–116, 142, 244
- DNS WhoIs, 143
- Domain Name Servers (DNS) system, 244, 263n31, 273n51, 276n88
- com and, 49, 51, 61–62, 273n53
- gov and, 49, 140
- ICANN and, 62
- mil and, 140
- net and, 62
- org and, 40
- purpose of, 48–49
- resolvers and, 51, 60–61
- root nameservers and, 49, 51, 53, 61–62
- security problems with, 51–52
- top-level domains and, 49, 62, 142
- xxx and, 142
- Donohue, Laura, 203
- DOS, 202
- Doyle, Arthur Conan, 43
- Drug dealers, 106, 137–138, 172, 184, 241
- Drug Enforcement Agency, 101
- Dumb terminals, 4, 6
- DuPont, 163

- Eavesdropping. *See* Surveillance; Wiretaps
- Ebadi, Shirin, 218
- eBay, 45, 123
- ECHELON, 152

- Economic Espionage Act, 153, 308n57
- Economic issues, 255
- communication networks and, 212–215
- Communications Assistance for Law Enforcement Act (CALEA)
- compliance and, 188–189
- cybersecurity and, 241–243
- insider attacks and, 163–164
- outsourcing and, 126, 154–157, 165, 198, 236
- spying and, 147–153, 165–171
- supply chains and, 154–157
- U.S. dominance and, 255
- value of communications security and, 215–219
- weather forecasts and, 154
- Einstein projects, 120–122, 219, 233
- Electronic Communications Privacy Act (ECPA), 80, 84, 99, 192–194
- Electronic Frontier Foundation (EFF), 45, 92, 132
- Electronic surveillance. *See* Bugs; Surveillance; Wiretaps
- Elliptic-Curve Diffie-Hellman, 47
- Elliptic-Curve Digital Signature Algorithm, 47
- Email, 7
- asynchrony of, 263n37
- bots and, 145
- communication network architectures and, 20–21, 24–32, 263n37, 268n88
- deep packet inspection and, 132
- design principles and, 41–42
- effectiveness of surveillance and, 102, 116, 121
- evolving communication technologies and, 124, 131–134, 137–139
- identifying intruders and, 145–146, 158, 164, 167–168
- as killer app, 20
- legal issues and, 72, 80–81, 87
- policy risks and, 220–222
- security risks and, 38, 41–42, 46–47, 52, 54, 58, 179, 191–194, 197, 252, 274n64
- sneak peeks and, 194
- spam and, 39, 54, 145–146
- U.K. Parliament and, 167
- Encryption, *See* Cryptography
- Endhosts, 146
- End-to-end design
- Internet and, 20, 31–32, 47, 59–60, 132, 195, 199, 222, 232, 236, 246, 249
- principle of, 31, 236
- Enigma, 44, 271n24
- E911, 85, 129–130
- Ericsson, 173, 198
- Escrowed Encryption Standard (EES), 114–115
- Essid, Chris, 231
- Estonia, xii, 53, 145, 146, 160, 171
- Estrada, Joseph, 30
- Ethane, 238–239
- European Commission, 63
- European Convention on Human Rights, 136–137, 203
- European Telecommunications Standards Institute (ETSI), 196
- Europol, 136–137
- Exigent letters, 193–195, 205, 207, 256, 323n98
- Export control, 116–119
- Facebook, 31, 138, 142, 191, 321n66
- Fairchild Semiconductor, 147, 163
- Faris, Iyman, 88
- Faxes, 72, 80, 132, 151, 195
- Federal Bureau of Investigation (FBI), 2–3, 256, 260n33
- Carnivore and, 85, 187, 196, 243, 245
- changes in law enforcement practice and, 142–143
- Communication Analysis Unit (CAU) of, 192–193, 205

- Federal Bureau of Investigation
 - (FBI) (cont.)
 - Communications Assistance for Law Enforcement Act (CALEA)
 - compliance and, 188
 - Computer and Internet Protocol Address Verifier (CIPAV) and, 133, 245, 249
 - cyberattacks and, 172
 - deep packet inspection (DPI) and, 219, 221
 - Digital Telephony proposal and, 81
 - economic espionage and, 150–151, 153
 - effectiveness of wiretapping and, 99–103, 106–112, 115, 118–119
 - evolving communication technologies and, 130, 133, 142–143, 302n34, 305n86
 - exigent letters and, 193–195, 205, 207, 256, 323n98
 - export control and, 118–119
 - Freeh and, 106
 - Hoover and, 68, 72–73, 95, 277n19, 278nn26,27
 - hot numbers and, 194
 - insider attacks and, 163–165
 - “interception and divulgence” ruling and, 175
 - interception capacity and, 82
 - intruder identification and, 150–153, 162–165, 172–174, 307n44, 311n97
 - Islamic radicals and, 211
 - journalists and, 205–206
 - King and, 69
 - legal issues and, 68–69, 72–75, 81–85, 90–92, 95
 - legislative oversight of, 68–69
 - Long and, 69
 - Magic Lantern and, 133
 - Mueller and, 112, 221
 - National Security Letter (NSL) and, 99–100, 103, 139, 192–194, 322n85
 - Pistole and, 92
 - policy risks and, 205–207, 211, 219, 221
 - post-cut-through dialed digits and, 82, 84
 - public perception of, 108
 - Quantico and, 143
 - right policy stance for, 240, 243–246, 249
 - rule of law and, 207–208
 - security risks and, 175, 187–188, 192–196
 - Sessions and, 317n6
 - sneak peeks and, 194
 - Soviet embassy tunnel and, 163
 - Special Agent in Charge (SAC) and, 192
 - spyware and, 133
 - telephone company contracts and, 193
 - Triggerfish and, 103, 248
 - VoIP and, 84–85
 - Watergate scandal and, 76
- Federal Communications Act, 67–70, 284n110
- Federal Communications Commission (FCC), 258n20, 269n101
 - Carterfone and, 5–6, 258n20, 259n21
 - communication during crises and, 227, 229
 - Communications Assistance for Law Enforcement Act, 84–85
 - evolving communication technologies and, 132, 300n18, 302n40
 - legal issues and, 238n103, 284n112
 - policy risks and, 219
 - right policy stance for, 243–245
 - SAFECOM and, 244–245
 - tariff 132 and, 259n21
 - telephone/computer convergence and, 128
 - VoIP and, 84–85

- Fermat integers, 124, 299n2
- Fiber optics, 22, 72, 87, 89, 123, 157, 176, 226–227, 306n18, 331n12
- Fifth Amendment, 11, 67
- File sharing, 34–35, 57, 132
- Firewalls, 55, 131, 159, 233–234, 238, 240, 265n59, 273n44
- First Amendment, 10, 78, 175–176, 192, 204, 218, 252, 316n3, 337n62
- First Energy, 161
- Fishing expeditions, 75
- Fitzgerald, Patrick, 106
- Flash drives, 146
- Flickr, 31
- Folding@home, 124–125
- Foreign Intelligence Surveillance Act (FISA), 65, 77–78, 84, 100, 281nn71,75
- Amendments Act and, 94, 192, 335n29, 336n41
- Court's Rules of Procedure and, 207–208
- excessive collection risks and, 192
- FISA Court rulings and, 90–93
- policy risks and, 207–208, 327n23, 335n29, 336n41
- President's Surveillance Program (PSP) and, 90–93
- Protect America Act and, 2, 93, 207, 240, 327n20, 336n41
- security risks and, 175, 189, 192, 194
- USA PATRIOT Act and, 86–87
- Foreign Service, 216
- 4ESS switch, 72, 181
- Fourth Amendment, 11
- Charles Katz v. United States*, 11, 70
- evolving communication technologies and, 127
- Goldman v. United States*, 70
- Irvine v. California*, 70
- Julius Silverman et al. v. United States*, 70
- Nardone v. United States*, 67–69
- Olmstead v. United States*, 67, 70
- policy risks and, 205, 250
- wiretaps and, 66–67, 70, 73, 75, 79, 90–92, 99, 205
- writs of assistance and, 66, 189–190
- Frames, 71–72
- France, 5, 258n16
- effectiveness of wiretapping and, 101
- evolving communication technologies and, 134–135, 141
- Internet security and, 42, 272n39
- intruder identification and, 148–152, 165, 173, 307n44
- legal issues and, 66
- policy risks and, 215, 217, 333n6
- Franklin, Benjamin, 66
- Freedom of Information requests, 102
- Freeh, Louis, 106, 283n108
- Frequency analysis, 44, 271n23
- Friendly circuits, 71
- Fromkin, David, 213
- Fuji, 149–150
- Fujitsu, 163
- Future Internet Design, 238
- Gacaca Courts, 207
- Gambling, 70, 73, 104, 106, 133
- Gamma Guppy intercepts, 135
- Gap, The, 155
- GE, 147
- General Dynamics, 147, 149
- General Services administration, 173
- General Union of Palestinian Students, 176
- Genovese crime family, 73, 130
- George, Dickie, 231
- Georgetown University, 256
- Georgia, 146, 171
- Germany, 5
- effectiveness of wiretapping and, 98, 109
- evolving communication technologies and, 134, 141

- Germany (cont.)
 Internet security and, 44, 270n17, 271n24
 intruder identification and, 147, 150–154, 167, 173
 legal issues and, 94, 278n27, 289n169
 policy risks and, 208, 222, 235, 237
- Gidari, Al, 101, 103, 190
- Gingrich, Newt, 178
- GNU General Public License, 268n97
- “Gold Bug, The” (Poe), 43
- Goldman v. United States*, 70
- Goldsmith, Jack, 90, 91
- Gonzales, Alberto, 91, 95
- Google, xi, 103, 315n160
 China and, 170
 Cloud computing and, 126, 220
 communication network architectures and, 31
 deep packet inspection (DPI) and, 219–222
 evolving communication technologies and, 123, 125–126, 142–143
 Gmail and, 47, 87, 121, 170, 222, 232, 301n27, 336n47
 Internet security and, 47, 49, 51, 59, 61, 273n51
 Iran and, 218
 policy risks and, 214, 218–222
 security risks and, 179–180
- Google Calendar, 126, 220
- Google Docs, 126
- Google Trends, 125
- Gorman, Siobhan, 119
- Government Emergency Telecommunications Service (GETS), 180, 226, 244
- Gov nameserver, 49, 140
- GPS technology, 130
- Greece, 3–4, 6, 177
 Athens Affair and, 177, 187, 234–235, 240–241
 Internet security and, 43
 intruder identification and, 164
 policy risks and, 217
 security risks and, 177, 185, 195, 217, 234–235, 240–241, 335n31
 Vodafone and, 177, 185, 234–235, 240–241
- Gregg, Judd, 2
- Gretag AG, 114–115
- Grinberg, Tomer, 109–110
- Griswold v. Connecticut*, 11
- Grumman, 147, 170
- GSM (Global System for Mobile Communications), 113
- Hackers, xii, 119, 196, 276n88
 China and, 166–169
 cyberattacks and, 8–9, 95, 145–146, 153, 168, 171, 208, 235–236, 333n7
 distributed denial-of-service (DDoS) attacks and, 53–55, 58, 120, 146, 161, 235
 evolving communication technologies and, 133
 intruder identification and, 157–161, 168
- Hager, Nicky, 152
- Hall, Paul, 109
- Hamas, 109
- Handshakes, 40–41, 53, 132
- Hanssen, Robert, 163, 165, 187
- Harman, Jane, 95
- Harris Corporation, 103
- Hashing, 47, 61, 237, 243–244, 272n38, 324n111, 337n57
- Hathaway, Melissa, 9
- Heartland Payment Services, 160
- Hellman, Martin, 45–46
- HEPNet, 21
- Hezbollah, 109
- Hitachi, 149
- Ho Chi Minh Trail, 136
- Hoffa, Jimmy, 69
- Holder, Eric, 212

- Holy Land Foundation (HLF), 109–110
Home Location Register (HLR), 26, 183
Honeywell, 149–150
Hoover, J. Edgar, 68, 72–73, 95,
277n19, 278nn26,27
Hot numbers, 194
Howard, Edward Lee, 162
HTMD, 211
Huawei, 168, 173
Hughes Aircraft, 149
Human perception, 65
HUMINT (human intelligence), 151
Hydrophones, 300n15
- IBM, 39, 147–149, 189, 196
Identity theft, 133, 234
Illegal search and seizure, 67–68
Immigrants, 108, 209–212
Immigration and Customs
Enforcement, 108
India, 43, 267n85, 295n78
communication networks role in
economic growth and, 214
intruder identification and, 150, 167,
314n137
policy risks and, 213–218, 223,
329n64
security risks and, 180, 235
Information Assurance Directorate
(IAD), 231–232
Information Sciences Institute (ISI), 27
Information technology (IT), 154–156
critical infrastructure risks and,
157–161
insider attacks and, 164–165
SCADA systems and, 158, 180–181,
239
Y2K and, 158
Infrastructure as a Service (IaaS), 126
Inman, Bobby, 216, 329n65
Insider attacks, 162–165
Instant Messaging (IM), 188, 252,
298n116
communication during crises and, 227
communication network architectures
and, 24–25, 30–31
design principles and, 41–42
evolving communication technologies
and, 140
Internet security and, 38, 41–42
Institute of Medicine, 97
Intel, xi, 268n94, 303n55
Intellectual property, 34–35, 149,
155–156, 170, 218, 280n52
Intellipedia, 143
“Interception and divulgence” ruling,
175
Interception capacity, 82
Interface Message Processors (IMPs), 19
International Telecommunications
Union, 62, 258n17
Internet
adoption of, 30
ARPANET and, 19–21, 27, 37–40,
263n40
availability and, 38–42
Baran and, 17–19, 28, 37–38
Berners-Lee and, 141
botnets and, 53, 145–146, 234, 305n2,
333n7
bursty traffic and, 17
business communication and, 37–38
caching and, 51–52, 63, 276n88,
331n12
censorship and, 218
cloud computing and, 53, 116,
125–127, 184, 228, 300n8, 301n27
Comprehensive National
Cybersecurity Initiative (CNCI) and,
120
critical infrastructure risks and,
157–161
cryptography and, 42–47 (*see also*
Cryptography)
cyberattacks and, 8–9, 95, 145–146,
153, 168, 171, 208, 235–236, 333n7

- Internet (cont.)
- Davies and, 17–19, 37–38
 - deep packet inspection and, 130–133
 - design principles of, 19–20, 37–42
 - development of, 17–21
 - distributed denial-of-service (DDOS) attacks and, 53–55, 58, 120, 146, 161, 235
 - Domain Name Servers (DNS) system and, 49–52, 60–63, 115–116, 142–143, 244, 263n31, 273n51, 276n88
 - end-to-end design of, 20, 31–32, 47, 59–60, 132, 195, 199, 222, 232, 236, 246, 249
 - governance shifts and, 141–142
 - grassroots communities and, 32
 - human values and, 238
 - IP addresses and, 20, 23–28, 42, 48–55, 58–61, 89, 120, 130–134, 140, 145, 179, 183, 186
 - Kahn and, 19–20
 - limitation of CALEA and, 246–248
 - malware and, 53–55, 120–122, 145, 181–182, 219–221, 234, 240, 312n111
 - mobility issues and, 133–134, 182–187
 - most popular sites on, 142
 - NAT boxes and, 127, 263n32, 300n11
 - network convergence and, 180–182
 - network hosts and, 22, 32, 40, 48–49, 53–58, 132, 141, 146, 167, 169, 219, 234, 239, 249, 336n47
 - network principles of, 19–20
 - packet-switching and, 3, 8, 18–19, 38, 56, 178
 - peering points and, 53, 89–90
 - peer-to-peer networking and, 18, 28, 34–35, 56–57, 132, 183, 260n33, 265n59, 269n101, 300n18
 - protocol stack and, 23–25
 - redundancy levels and, 18
 - reliability and, 38–42
 - root nameserver and, 49, 51, 53, 61–62
 - routing and, 3–4, 19–30, 48, 52–53, 57–60, 86, 127, 139–140, 169, 173, 178, 183–186, 190, 199, 234, 238–239, 251
 - security efforts in, 60–63
 - security risk of, 38–39, 51–53, 178–179 (*see also* Security)
 - spam and, 39, 54, 145–146
 - spoofing and, 52–55, 58, 60–61, 113, 187, 196
 - TCP/IP and, 20, 23–25, 37–42, 46, 53, 56, 132–133, 264nn50,51, 269n3
 - 32-bit address space and, 20, 62
 - transactional information and, 59–60
 - Trojan horses and, 54, 94, 146, 166–167, 170
 - viruses and, 39, 53–55, 57, 124, 133, 145–146, 168, 197, 274nn63,64
 - VoIP and, 84–85 (*see also* Voice over Internet Protocol (VoIP))
 - walled garden approach and, 22
 - worms and, 47–48, 53–55, 145, 159, 234, 273n44
 - zones and, 49, 51, 61, 142, 273nn47,51
- Internet Activities Board, 238
- Internet Corporation for Assigned Names and Numbers (ICANN), 62, 142
- Internet Engineering Task Force (IETF), 142, 195, 197, 251
- Internet Explorer, 170
- Internet Relay Chat, 140
- Internet service providers (ISPs), 4, 330n81
- communication network architectures and, 24, 31, 263n34
 - deep packet inspection and, 130–133, 219–222
 - evolving communication technologies and, 130–132, 136, 140
 - functionality during crises and, 226–227

- legal issues and, 80, 85–86, 89, 284n114
 security and, 51, 55, 176, 183–187, 197
 IP addresses, 120, 145
 communication network architectures and, 20, 23–28, 264n48, 265n59
 DNSSEC and, 52, 60–62, 115–116, 142, 244
 Domain Name Servers (DNS) system and, 49–52, 60–63, 115–116, 142–143, 244, 263n31, 273n51, 276n88
 evolving communication technologies and, 130–134, 140
 legal issues and, 89
 mapping and, 48–49, 137–138, 248
 mobile communications and, 25–27, 183–185
 number designations of, 20
 security and, 42, 48–55, 58–61, 179, 183, 186, 273n48, 275n80, 276n88, 317n15
 iPhones, 4, 6–7, 33, 99, 127, 134, 230
 iPods, 154, 155–157, 173
 IPsec, 62–63, 119
 IPv6 (Internet Protocol version 6), 20, 62–63, 132, 244
 Iran, 170, 215–216, 218
 Iraq, 119, 171
 Irish Republican Army (IRA), 206–207
Irvine v. California, 70
 Isamuddin, Riduan, 112
 Ishikawajima-Harima Heavy Industries, 150
 Israel, 135, 141, 149–150, 171, 235

 Jackson, Robert, 68, 201–202
 Japan
 effectiveness of wiretapping and, 107, 113, 297n113
 evolving communication technologies and, 135, 141–142, 149–151, 154, 163, 173
 Internet security and, 49, 63
 security risks and, 189, 198, 255–256, 325n131
 texting and, 29
 Japanese External Trade Organization, 149
 Japanese Navy, 107
 Jefferson, Thomas, 1, 66
 Jennings, Dennis, 38, 42
 Jihadists, 109, 209–211
 Jintao, Hu, 214
 Johns Hopkins University, 179
 Johnson, Lyndon B., 69, 73
 Journalists, 2, 10, 260n40, 304n76.
 See also Specific newspaper
 Code of Federal Regulations and, 204–205
 court testimony and, 204
 ECHELON and, 152
 First Amendment and, 204, 252, 337n62
 Nixon and, 69
 right policy stance for, 252–253
 Watergate scandal and, 76
 wiretaps and, 68–69, 76–77, 94, 164, 204–208, 217, 337nn62,63
 Judt, Tony, 223
Julius Silverman et al v. United States, 70

 Kahn, David, 134
 Kahn, Robert, 19–20, 23–24, 31, 37–39, 48
 Kaminsky, Dan, 276n88
Kansas v. Colorado, 200
 Karn, Philip, 116
 Kassir, Oussama, 109
 Kennedy, John, 278n27
 Kerckhoffs, Auguste, 43
 Keyboards, 133, 202, 325n138
 Key loggers, 94, 133, 302n34
 Keys, 41, 94, 271n19
 Advanced Encryption Standard (AES) and, 45–47, 231, 272n36
 brute-force decryption and, 114, 237, 249, 257n4, 271n27, 324n111

Keys (cont.)

- Caesar cipher and, 43
- Clipper and, 114–115, 195–196
- Data Encryption Standard (DES) and, 44–45, 47, 114–115, 244, 257n4
- Diffie and, 45–46
- Enigma and, 44, 271n24
- escrowed, 114–115, 116–117
- evolving communication technologies and, 139–140
- Hellman and, 45–46
- length of, 44–45, 114, 117, 272n36
- Mauborgne and, 44
- Moore’s law and, 45
- nonrepudiation and, 46, 60
- one-time pad and, 44
- polyalphabetic substitution ciphers and, 44
- private, 45–46, 61, 297n106, 304n71
- public, 45–47, 61, 139, 297n106, 304n71
- rotor machines and, 44
- Scherbius and, 4
- signatures and, 46–47, 61–62, 281n65
- Skipjack and, 114–115
- symmetric, 45
- Vernam and, 44
- KGB, 147, 162, 165
- Khalid Sheikh Mohammed, 98
- Khalil, Naji Antoine Abi, 109–110
- Kidnapping, 71, 100, 105–107
- Killer apps, 20
- King, Martin Luther, Jr., 69
- Kissinger, Henry, 147
- Klein, Mark, 89, 176–177
- Kodak, 150
- Kollar-Kotelly, Colleen, 92
- Korea, 63, 150, 154, 166, 173, 189, 215
- Ku Klux Klan, 208

- Lamberth, Royce, 92
- Land Mobile Radio (LMR) systems, 229–231
- Langley, 143
- La Porta, Thomas, 180
- Laser microphones, 249, 337n53
- Latitude, 103
- Legal issues. *See also* U.S. Supreme Court
 - antecedents for wiretapping law and, 66–70
 - Authorization for Use of Military Force (AUMF) and, 93
 - authorized spyware and, 133
 - Bill of Rights and, 1, 10, 67, 189–190
 - black-bag jobs and, 71, 133
 - Bloody Sunday and, 206–207
 - Brazenburg v. Hayes*, 204
 - bugs and, 9, 69, 70, 104, 106, 197, 249
 - Charles Katz v. United States*, 11, 70
 - Church Committee and, 60, 69, 77, 175
 - City of Ontario, California et al., Petitioners v. Jeff Quon*, 121
 - civil rights and, 69, 73, 97, 175
 - Code of Federal Regulations and, 204–205
 - consensual overhear and, 71, 106
 - court orders and, 71, 79–81, 84, 89–90, 99–104, 136, 177, 184, 186
 - current law on wiretaps, 242–243
 - deep packet inspection and, 130–133, 219–222
 - Digital Telephony proposal and, 81
 - Electronic Communications Privacy Act (ECPA) and, 80, 84, 99, 192–194
 - “electronic surveillance” term and, 69
 - excessive collection risks and, 189–195
 - exigent letters and, 193–195, 205, 207, 256, 323n98
 - Federal Communications Act and, 67–70, 284n110
 - Fifth Amendment, 11, 67
 - First Amendment, 10, 78, 175–176, 192, 204, 218, 252, 316n3, 337n62

- fishing expeditions and, 75
 Foreign Intelligence Surveillance Act (FISA) and, 65, 77–78, 84, 86–87, 90–94, 100, 189, 192, 194, 207–208, 281n71, 75, 327n23, 335n29, 336n41
 Fourth Amendment, 11, 66–67, 70, 73, 75, 79, 90–92, 99, 127, 189–190, 205, 250
 gambling and, 70, 73, 104, 106, 133
Goldman v. United States, 70
 hot numbers and, 194
 human perception and, 65
 illegal search and seizure and, 67–68
 “interception and divulgence” ruling and, 175
Irvine v. California, 70
Julius Silverman v. United States, 70
Kansas v. Colorado, 200
 minimization requirement and, 74
 modern networks and, 78–85
NAACP v. Alabama, 11
Nardone v. United States, 67–69
Olmstead v. United States, 11–12, 67, 70
 Omnibus Crime Control and Safe Streets Act and, 65, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
 organized crime and, 8–9, 66, 72–73, 97, 106, 130, 164, 172, 312n111
 pen registers and, 79–86, 89, 99–104, 133, 137, 187, 190, 194, 196, 219, 248, 285n120, 292n31, 337n63
 post-cut-through dialed digits and, 82, 84
 Preamble of Constitution and, 200–201
 President’s Surveillance Program (PSP) and, 90–95, 112, 200, 243, 252, 256, 286n137, 338n3
 probable cause and, 11, 74, 77–78, 157, 337n63
 Prohibition Era and, 66–68
 Protect America Act (PAA) and, 2, 93, 207, 240, 327n20, 336n41
 Radio Act and, 67
 right policy stance for, 250–253
Roe v. Wade, 11
 rule of law, 206–208
 search warrants and, 2–3, 66, 70, 79–80, 133, 207, 260n47, 279n47
Smith v. Maryland, 79–80, 99
 sneak peeks and, 194
Stengart v. Loving Care Agency, 298n122
 subpoenas and, 79, 94, 99, 102, 192–193, 204–205, 305n86, 337n63
Tash Hepting et al. v. AT&T Corporation et al., 92–93, 176
 Telecommunications Act and, 89, 181
 Tenth Amendment, 200
 Title III order, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
 traffic analysis and, 134–139
 two-party consent and, 71
 ubiquitous networks and, 233–234
Uniformed Sanitation Men v. Commission of Sanitation, 105
United States v. Miller, 79
United States v. Poeta, 105
United States v. United States District Court for the Eastern district of Michigan et al., 75
 USA PATRIOT Act, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
 U.S. Department of Justice (DoJ) and, 68, 75, 90–92, 277n21, 280n56
U.S. Term Limits, Inc. v. Thornton, 200
 VoIP and, 2, 129–130
 wiretaps and, 65–95, 204–206
 writs of assistance and, 189–190
Youngstown Sheet & Tube Co. v. Sawyer, 90
 Letters
 exigent, 193–195, 205, 207, 256, 323n98
 written, 1, 13, 66, 94, 123, 170, 193–195, 205–208, 220, 256

- Li and Fung, 155
- Lichtblau, Eric, 94
- Life* magazine, 69
- Limited, The, 155
- Link layer, 23
- Linux, 32–34, 268nn95,97, 274n66
- Loan-sharking, 73
- Local exchange, 14, 16, 78
- Local loop, 71–72, 81–82
- Location Areas, 26
- Location tracking, 26–27, 58, 248, 252.
 - See also Traffic Analysis; Transactional information
 - Communications Assistance for Law Enforcement Act (CALEA) and, 84
 - deep packet inspection and, 131
 - disguising, 7, 81
 - GPS and, 130
 - Internet, 20, 25–26, 89–90, 183–184
 - perception of anonymity and, 98
 - RFID tags and, 259n29
 - scanners and, 259n29
 - signal strength and, 134
 - telephones and, 7, 14, 25–27, 107, 129–130, 178, 182–185, 197
 - transactional information and, 99–104
 - VoIP and, 85, 137
- Lockheed, 149
- London bombings, 138, 267n85
- London Metropolitan Police, 211
- London Sunday Times*, 69
- Long, Edward, 69
- Long-distance providers, 4, 39–40, 82, 88, 236, 279n45
- Looming Tower, The: Al Qaeda and the Road to 9/11* (Wright), 94
- Loop extenders, 71
- Lord, William, 169
- Lott, Trent, 268n87
- Lotus Notes, 116–117

- Maclean, Donald, 163, 311n103
- Madrid train bombing, 209
- Magic Lantern, 133
- Mak, Chi, 169, 314n152
- Malware
 - cybersecurity and, 53–55, 120–122, 145, 181–182, 219–221, 234, 240, 312n111
 - host attacks and, 53–55
 - Trojan horses and, 54, 94, 146, 166–167, 170
- March on Washington, 68
- Marcus, Scott, 176
- Marion, Pierre, 148–149
- Martinez, Jorge de los Reyes Butista, 110
- Martin Marietta, 149
- Martus, 217–218
- Mary, Queen of Scots, 1
- Massachusetts Institute of Technology (MIT), 138
- Massively multiplayer online role-playing games (MMORPGs), 188–189
- MasterCard, 172
- Mauborgne, Joseph, 44
- McCarthyism, 10
- McDaniel, Patrick, 180
- McDonnell Douglas, 149
- McVeigh, Timothy, 209
- Meetup.com, 31
- Melissa virus, 54, 274n64
- Melo, Jose Tito Libio Ulloa, 110
- Mesopotamia, 43
- Metcalfe's law, 32
- Mexico, 141, 218
- Meyrrose, Dale, 143
- MFENet, 21
- Microsoft, xi, 33
 - DOS, 202
 - Excel, 274n64
 - Hotmail, 87
 - Network, 142
 - Outlook, 274n64
 - Vista, 202, 274n66, 325n136
 - Windows, 202, 274n61
 - Word 97, 274n64

- Microwave transmissions, 135, 147–148
- Mil namserver, 140
- Min, Gary, 163
- Minimization, 74, 78
- Mitsubishi, 150
- Mobile Switching Center (MSC), 129, 183, 248
- Mockapetris, Paul, 49
- Moon, Jae Yun, 33
- Moore's law, 45
- Morris worm, 47–48, 54, 145
- Morse code, 13, 271n19
- Mosabbah, Abdel Rahman, 211
- MoveOn organization, 32, 268n88
- Mueller, Robert, 112, 221
- Murphy's law, 195–198
- Murrah Building, 209, 222
- Mutually Assured Destruction, 215
- NAACP v. Alabama*, 11
- Nagaraja, Shishir, 138, 191
- Nagin, Ray, 228
- Naipaul, V. S., 214
- Naral Pro-Choice America, 132
- Narayanan, Arvind, 191
- Nardone, Carmine, 67–69
- Narus machines, 176
- NASA, 34, 55, 169, 234
- National Infrastructure Policy Plan, 157
- National Institute of Standards and Technology (NIST), 45, 179, 243–244
- National Physical Laboratory, 17
- National Research Council, 8–9, 97, 98, 153, 163, 169, 208, 219, 237, 252
- National Science Foundation (NSF), 39, 47, 238
- Advanced Encryption Standard (AES) and, 46
- Future Internet Design and, 21–22
- Jennings and, 38, 42
- network hierarchy and, 38
- NSFNET and, 21–22, 38, 42, 264n46, 334n20
- Office of Advanced Scientific Computing and, 38
- supercomputing sites and, 141
- National Security Agency (NSA), 2, 216, 281n75
- Advanced Encryption Standard (AES) and, 46–47
- Baker and, 297n113
- Clipper and, 114–115
- communication during crises and, 231–232
- effectiveness of wiretapping and, 107, 114, 117–121, 290n7
- Einstein projects and, 120–122
- evolving communication technologies and, 134–136, 147–148, 302n46, 305n87
- excessive collection risks and, 192
- export control and, 118–119
- Gamma Guppy intercepts and, 135
- Internet and, 39, 46–47, 270n9
- interoperability and, 231
- intruder identification and, 163, 173
- military communications equipment and, 198
- Narus machines and, 176
- Office of Munitions Control and, 114
- public network traffic and, 119–122
- right policy stance for, 241–246
- security risks from wiretapping and, 175–177, 192, 197–199, 316n1
- SHAMROCK program and, 316n1
- Skipjack and, 114–115
- Soviet embassy tunnel and, 163
- Suite B algorithms and, 47, 231–232
- traffic analysis and, 134–139, 176–177
- warrantless wiretaps and, 87–94
- watchlists of, 175
- National Security Law Branch, 194
- National Security Letter (NSL), 99–100, 103, 139, 192–194, 322n85
- National Security Presidential Directive 54, 120

- NATO, 167
- Natural disasters, 267n85, 331nn1,5
communications effects of, 225–231
death tolls from, 223
Information Assurance Directorate (IAD) and, 231–232
Land Mobile Radio (LMR) systems and, 229–231
- Navajo code talkers, 45
- Naval Ocean Systems Center, 166
- Nebuad, 131
- Negroponte, John, 143
- Net nameserver, 62
- Network Address Translation (NAT)
boxes, 127, 263n32, 300n11
- Network effect, 125, 241
- Network Working Group, 195, 197
- Newton's laws of motion, 124–125
- New Yorker*, 94, 139
- New York Police Department (NYPD), 209–211
- New York Stock Exchange (NYSE), 157
- New York Times*, 2, 69, 87–88, 91, 94–95, 145, 175–176, 205, 220, 228, 260n40
- New Zealand, 59, 113, 141, 152, 167, 235
- Nigeria, 211
- NIPRNet, 169
- Nissan, 150
- Nissenbaum, Helen, 233
- Nixon, Richard M., 69, 76
- Nokia, 13
- Nongovernmental organizations (NGOs), 216–217
- Nonrepudiation, 46, 60
- Northeastern University, 138
- Northern Ireland, 206–207, 326n12
- Northrop Grumman, 170
- NSFNET, 21–22, 38, 42, 264n46, 334n20
- Nuclear energy, 141, 157, 159, 165
- Nuclear weapons, 17, 147, 163, 171, 208, 215–216, 256
- Obama, Barack, 9
- O'Brien, Lawrence, 76
- Ohm, Paul, 219–220
- Olmstead, Roy, 11–12, 67, 70
- Olmstead v. United States*, 11–12, 67, 70
- Omnibus Crime Control and Safe Streets Act
establishment of, 65
Title III order and, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
- One-time pad, 44
- Onion routing, 139–141, 275n84
- OpenFlow, 238–239
- Open source software, 56, 123, 217, 269n99
communication network architectures and, 31–33
GNU General Public License and, 268n97
Linux and, 32–33, 268nn95,97, 274n66
- Oracle, 155, 191
- Organized crime, 8–9, 164, 172, 312n111
effectiveness of wiretapping and, 97, 106
gambling and, 70, 73, 104, 106, 133
Genovese family and, 73, 130
Hoover's denial of, 72–73
loan-sharking and, 73
local law enforcement and, 73
Prohibition Era and, 66, 73, 259n31
prostitution and, 73, 104
spyware and, 133
structure of, 73
victimless crimes and, 73
- Org nameserver, 40
- Osman, Hussain, 138–139

- Otis, James, Jr., 190
- Out-of-band signaling, 29, 40
- Outsourcing, 126, 154–157, 165, 198, 236
- Oxfam America, 176
- Ozzie, Ray, 117, 297n106
- Packets, 300nn8,17
- anonymization tools and, 139–141, 191, 222, 321n64
 - communication network architectures and, 18–25, 29, 264nn48,50,51, 269n7
 - cyberattacks and, 146 (*see also* Cyberattacks)
 - Davies and, 19
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - design principles and, 37–42
 - effectiveness of surveillance and, 120–121, 125, 129–132, 141
 - handshakes and, 40–41, 53, 132
 - Internet security and, 38–41, 48, 53, 55–62
 - intruder identification and, 146, 160
 - legal issues and, 78, 85
 - limitation of CALEA and, 246–248
 - network layers and, 22–25
 - policy risks and, 219–221, 233, 236, 239–241, 246–248, 334n20
 - protocol stack and, 23–25
 - Quality of Service (QoS), 334n20
 - routing and, 4, 20–30, 48, 57, 59, 86, 139–140, 183, 185, 190, 234, 238–239
 - security risk of, 178–179, 183–186, 199, 318n26
 - sniffers and, 53, 85, 160, 178–179, 199
 - TCP/IP and, 25
 - traffic analysis and, 134–139
 - Tutelage and, 219
 - Packet-switching, 3, 8, 18–20, 38, 56, 178
- Padilla, Jose, 110
- Pakistan, 98, 109, 111, 172, 211
- Palestinians, 176, 211, 223, 317nn7,9
- PANS (Pretty Advanced Network Services), 4
- Paracha, Uzair, 109
- Passwords
- Cisco architecture risks and, 196–197
 - easily guessed, 178
 - Internet security and, 48, 52, 54, 58, 169, 237, 273n59, 276n88, 298n122, 3336n47
 - usernames and, 58, 169, 179, 197, 324n111
- Patches, 35, 48, 56, 63, 166, 170, 227, 276n88
- Patents, 31, 149, 261n3
- Path Intelligence Ltd., 103
- Paul, Christopher, 109
- PayPal, 52
- Pearl Harbor, 255
- Peering points, 53, 89–90
- Peer-to-peer, 260n33
- communication network architectures and, 18, 28, 34–35, 265n59, 269n101
 - evolving communication technologies and, 132, 300n18
 - file sharing and, 34–35, 57, 132
- Pen registers
- Computer and Internet Protocol Address Verifier (CIPAV) and, 133
 - court orders and, 101–103
 - data on use of, 102
 - deep packet inspection (DPI) and, 130–133, 219–222
 - Department of Justice and, 101–102
 - effectiveness of surveillance and, 99–104, 292n31
 - evolving communication technologies and, 133, 137

- Pen registers (cont.)
 excessive collections risks and, 190, 194
 legal issues and, 79–86, 89, 99–104, 285n120
 order expiration and, 101
 policy risks and, 219
 post-cut-through dialed digits and, 82, 84
 real-time access and, 99–102
 security risks and, 187, 190, 194, 196, 248, 337n63
 spyware and, 133
 transactional information and, 99–104
 underreporting on, 101–102
 U.S. Marshals Service and, 100
- Perkins Coie LLP, 101
- Persia, 43
- Personal identification numbers (PINs), 160, 172, 242
- Philbin, Patrick, 90
- Philby, Kim, 162–163, 311n103
- Phishing attacks, 52, 58
- Phone cards, 7, 72, 98
- Phone phreaks, 270n12
- Photo-sharing, 31
- Physical layer, 23
- Pistole, John, 92
- Plant, Sadie, 266n65
- Platform as a Service (PaaS), 126
- Poe, Edgar Allen, 43
- Points-of-Presence (POP), 226–227
- Polyalphabetic substitution ciphers, 44
- PortalPlayer, 154
- Port number, 131, 274n67
- Postal service, 66, 157, 186, 212
- Post-cut-through dialed digits, 82–83
- POTS (plain old telephone service), 4
- Power grid failure, 160–161
- Power, Samantha, 208
- Predator drone, 107
- President's Surveillance Program (PSP), 90–95, 112, 200, 243, 252, 256, 286n137, 338n3
- Prime numbers, 45–46, 124, 299n2
- Privacy, 3, 6, 11, 58, 312n115
 anonymization tools and, 139–141, 191, 222, 321n64
 Carnivore and, 85, 187, 196, 243, 245
Charles Katz v. United States and, 11, 70
 communication network architectures and, 30, 35, 266n65
 cryptography and, 1–2, 42–47 (*see also* Cryptography)
 deep packet inspection and, 130–133, 219–222, 234–235, 240–241
 effectiveness of surveillance and, 97, 99, 101, 105, 113, 120–122, 298nn122,123, 299n126
 Einstein projects and, 120–122, 219, 233
 Electronic Communications Privacy Act (ECPA) and, 80, 84, 99, 192–194
 Europol and, 136–137
 evolving communication technologies and, 132, 136, 139–141, 304n70
 expectation of, 79
Griswold v. Connecticut and, 11
 identity theft and, 133, 234
 journalists and, 2, 10, 68–69, 76–77, 94, 164, 204–205, 208, 217, 252–253, 260n40, 304n76, 337nn62,63
 legal issues and, 65–67, 74, 78–81, 84–85, 93–94
 Martus and, 217–218
 minimization requirement and, 74
NAACP v. Alabama, 11
 Olmstead, Roy and, 11
 onion routing and, 139–141, 275n84
 policy risks and, 212, 214, 217–222, 326n2
 postal service and, 66, 157, 186, 212
 President's Surveillance Program (PSP) and, 90–95, 112, 200, 252, 256, 286n137, 338n3
 probable cause and, 11, 74, 77–78, 157, 337n63

- Prohibition Era and, 66–68
 right policy stance for, 250–253
 right to, 10
Roe v. Wade, 11
 search warrants and, 66, 70, 79–80, 133, 207, 260n47, 279n47
 security risks and, 182, 189–192, 199, 238, 244, 250, 252, 321n64
Smith v. Maryland, 79–80, 99
 telegraph and, 212
 traffic analysis and, 133–139
 transactional information and, 59–60, 72, 78, 82, 103 (see also Transactional information)
 USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
 wiretaps and, 65–66 (see also Wiretaps)
- Privacy on the Line: The Politics of Wiretapping and Encryption* (Diffie and Landau), 65
- Private key cryptography, See Public key cryptography
- Probable cause, 11, 74, 77–78, 157, 337n63
- Prohibition Era, 66–68, 73, 259n31
- Protect America Act (PAA), 2, 93, 207, 240, 327n20, 336n41
- Protein folding, 124–125, 300n5
- Protocol stack, 23–25
- PTTs (Public Telegraph and Telecommunications), 42
- Public key cryptography, 45–47, 61, 139, 297n106, 304n71
- Public Safety Answering Points (PSAPs), 129
- Public Switched Telephone Network (PSTN), 4–6, 39, 47, 157
 blue box attacks and, 39–40, 196, 270n12
 communication network architectures and, 13, 18–30, 34, 262n19, 263n31, 267n84
 critical infrastructure risks and, 157
 decentralized networks and, 19–20
 deep packet inspection and, 132
 evolving communication technologies and, 128–129, 132, 142
 layers of, 22
 legal issues and, 78, 85
 Mobile Switching Center and, 129, 183, 248
 network convergence and, 180–182
 out-of-band signaling and, 29, 40
 redundancy and, 18
 routing tables and, 24
 security risks and, 178–187, 202, 317n15
 telephone/computer convergence and, 128–130
 usage of, 30
 voice quality and, 30–31
- Quality of Service (QoS) packets, 334n20
- Quantico, 143
- Quest, 88
- QWERTY keyboard, 202, 325n138
- Race riots, 73
- Radio, 4–5, 44, 258n20, 270n17, 291n26, 336n37
 cell phones and, 113
 communication during crises and, 226, 228–232
 communication network architectures and, 17, 26, 31
 cryptography and, 43
 evolving communication technologies and, 127–128, 133–136
 hackers and, 157
 intruder identification and, 157–159, 173
- Land Mobile Radio (LMR) systems and, 229–231
 legal issues and, 67–71, 78, 80, 87, 282n86

- Radio (cont.)
 - RFID tags and, 7, 127–128, 180–181, 259n29
 - security risks and, 178, 186, 198
 - signals from space and, 124
 - traffic analysis and, 134–136
- Radio Act, 67
- Radio Shack, 115, 231
- Railroads, 4, 13–14
- RAND, 17, 216–217
- Raytheon, 173
- RBS WorldPay, 160
- RCA International, 148
- Recon Optical, 149, 235
- Redundancy levels, 17–18, 21, 40, 270n13, 273n48
- Reed's law, 32
- Regional networks, 21, 27, 38, 87
- Regulation of Investigatory Powers Act (RIPA), 327n21
- Remote delivery, 187–188
- Repeaters, 16, 230
- Republic of Ireland, 207
- Resource-sharing, 19–20
- RFID (radio-frequency ID) tags, 7, 127–128, 180–181, 259n29
- Risen, James, 94
- Roberts, Lawrence, 19
- Roe v. Wade*, 11
- Roosevelt, Franklin D., 68
- Rootkits, 146, 177
- Root nameservers, 49, 51, 53, 61–62
- Rotor machines, 44, 271n23
- Routers, 3
 - Cisco, 6, 52, 173, 196, 235, 241, 243, 274n61, 316n176, 324n114, 335n31, 337n57
 - communication network architectures and, 19–24, 263nn31,34, 264n48
 - description of, 23–24
 - evolving communication technologies and, 127
 - intruder identification and, 169, 173
 - security issues and, 48, 52–53, 60, 178, 184–186, 199, 238, 251, 274n61, 324n114
 - updating and, 48
- Routing, 4
 - best-effort basis and, 24
 - communication network architectures and, 20–30, 262n15, 263nn31,34, 264n48
 - cost of, 24
 - evolving communication technologies and, 139–140
 - layers of, 22–25
 - legal issues and, 86
 - onion, 139–140, 275n77
 - protocol stack and, 23–25
 - PSTN, 20
 - security issues and, 48, 57, 59, 183, 185, 190, 234, 238–239, 275n77
 - texting and, 30
 - VoIP and, 27–28, 28
- Routing tables, 24, 48, 263n31, 264n48
- Roving wiretaps, 80–81, 86, 130, 172
- RSAREF, 116
- RSS feeds, 31
- Rubinfeld, Jed, 189–190
- Rule of law, 206–208
- Russia, 98
 - Ames, Aldrich, 98
 - communication networks role in economic growth and, 213
 - intruder identification and, 146, 160, 170–171
 - policy issues and, 213
 - terrorists, 223
- Rwanda, 207
- SAFECOM, 244–245
- Samsung, 154
- Santa Fe Institute, 138
- Satellite phones, 107, 228
- Scanners, 178, 182, 259n29
- Scarfo, Nicodemo S., 133

- Scherbius, Arthur, 44, 271n24
- Schneier, Bruce, xii
- Schwartz, Herman, 105
- Script kiddies, 145
- Search warrants, 66, 79–80, 133, 207, 260n47
- Foreign Intelligence Surveillance Act and, 77–78
- Omnibus Crime Control and Safe Streets Act and, 65, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
- spyware and, 133
- USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- warrantless wiretaps and, 2–3, 67–78, 87–95, 175–176, 187, 192, 203–204, 207, 212, 223, 240, 243, 246, 252, 336n41, 338n3
- Second Life* (online game), 188–189
- Secret Power: New Zealand's Role in the International Spy Network* (Hager), 152
- Secret Service, 108
- Secure Hash Algorithm, 47
- Security
- authentication and, 34, 40–41 (*see also* Authentication)
 - blue box attacks and, 39–40, 196, 270n12
 - built-in, 198–200
 - business models and, 55
 - caching and, 51–52, 63, 276n88, 331n12
 - Cisco architecture risks and, 196–197
 - cloud computing and, 53, 116, 125–127, 184, 228, 300n8, 301n27
 - Communications Assistance for Law Enforcement Act (CALEA) and, 188–189, 246–248
 - Comprehensive National Cybersecurity Initiative (CNCI) and, 120
 - Computer and Internet Protocol Address Verifier (CIPAV) and, 133, 245, 249
 - Computer Security Act and, 244
 - creating long-term risk and, 200–202, 251, 253
 - critical infrastructure risks and, 157–161
 - cryptography and, 42–47 (*see also* Cryptography)
 - cybersecurity and, 9, 95, 120 (*see also* Cybersecurity)
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - Department of Defense and, 6, 19, 119, 150, 153, 286nn137,142, 338n3
 - design principles for, 38–39
 - Domain Name Servers (DNS) system and, 49–52, 60–63, 115–116, 142–143, 244, 263n31, 273n51, 276n88
 - domestic communications and, 147–148
 - Einstein projects and, 120–122, 219, 233
 - end-to-end encryption and, 47, 57–60, 179, 195, 199, 222, 232, 246, 249, 336n47
 - excessive collection risks and, 189–195
 - export control and, 116–119
 - firewalls and, 55, 131, 159, 233–234, 238, 240, 265n59, 273n44
 - fishing expeditions and, 75
 - frequency analysis and, 44, 271n23
 - handshakes and, 40–41, 53, 132
 - hashing and, 47, 61, 237, 243–244, 272n38, 324n111, 337n57
 - identity theft and, 133, 234
 - journalists and, 2, 10, 68–69, 76–77, 94, 164, 204–205, 208, 217, 252–253, 260n40, 304n76, 337nn62,63
 - keys and, 41, 43–47 (*see also* Keys)

Security (cont.)

- long-distance telephone calls and, 4, 39–40, 82, 88, 236, 279n45
- malware and, 53–55, 120–122, 145, 181–182, 219–221, 234, 240, 312n111
- mobile communication risks and, 182–187
- Moore's law and, 45
- Morris worm and, 47–48, 54, 145
- Murphy's law and, 195–198
- Mutually Assured Destruction and, 215
- national security cases and, 65, 68–69, 72, 75–77, 87, 91–93, 97–99, 103–108, 111, 120, 122, 175, 194, 208, 215–218, 223
- National Security Presidential Directive 54 and, 120
- natural disasters and, 223, 225–226
- network convergence and, 180–182
- network layers and, 22–25
- nuclear weapons and, 17, 147, 163, 171, 208, 215–216, 256
- operating systems and, 32–34, 52, 54, 56, 133, 146, 182, 202, 242, 274nn64,66, 335n24
- organized crime and, 8–9, 66, 72–73, 97, 106, 130, 164, 172, 312n111
- out-of-band signaling and, 29, 40
- passwords and, 48, 52, 54, 58, 169, 178, 197, 237, 273n59, 276n88, 298n122, 324n111, 336n47
- patches and, 35, 48, 56, 63, 166, 170, 227, 276n88
- protocol stack and, 23–25
- random malice and, 39
- remote delivery risks and, 187–188
- right policy stance for, 233–253
- root nameserver and, 49, 51, 53, 61–62
- routers and, 3, 19–20, 22–24, 48, 52–53, 60, 127, 169, 173, 178, 184–186, 199, 238, 251
- September 11 attacks and, xi, 2, 85–86, 88, 93, 97–98, 108, 136, 143, 158, 191, 193, 206–210, 222–228
- Slammer worm and, 159, 234
- spoofing and, 52–55, 58, 60–61, 113, 187, 196
- terrorists and, 2 (*see also* Terrorists)
- traffic analysis and, 133–139
- transactional information and, 59–60, 72, 78, 99–101, 103 (*see also* Transactional information)
- Trojan horses and, 54, 94, 146, 166–167, 170
- USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- usernames and, 58, 169, 179, 197, 324n111
- value of communications security and, 215–219
- VeriSign and, 62
- virtual private networks and, 46, 119, 179, 233, 336n47
- viruses and, 39, 53–55, 57, 124, 133, 145–146, 168, 197, 274nn63,64
- walled garden approach and, 22
- worms and, 47–48, 53–55, 145, 159, 234, 273n44
- zones and, 49, 51, 61, 142, 273n47, 273n51
- Security and Freedom through Encryption Act, 118
- Security theater, xi–xii
- Seed data, 191
- Senate Select Committee to Study Governmental Operations. *See* Church Committee
- September 11 attacks, xi, 2
 - communications effects of, 226–229
 - effectiveness of surveillance and, 97–98, 108
 - evolving communication technologies and, 136, 143
 - intruder identification and, 158

- legal issues after, 85–88, 93
- Pentagon and, 222
- policy risks from wiretapping and, 206–210, 222–223
- security risks from wiretapping and, 191, 193
- slow CIA response to, 284n117
- wiretaps after, 85–87
- World Trade Center and, 222, 226, 228–229
- Sessions, William, 317n6
- SETI@home, 124–125
- SHAMROCK program, 316n1
- Shareef, Derrick, 110
- Shay's Rebellion, 201
- Shirky, Clay, 32
- Shmatikov, Vitaly, 191
- Signaling systems, 4–5
 - System 6 (SS6), 29, 39
 - System 7 (SS7), 29, 79–80, 180–181, 265n62, 266n71
- Signatures
 - cryptography and, 46–47, 61–62, 281n65
 - digital, 46–47, 61–62, 281n65
 - guarantees and, 62, 276nn86,87
 - notarized, 62
- Skipjack, 114–115
- Skype, 4, 6, 28, 119, 260n33
 - communication during crises and, 232
 - deep packet inspection and, 222
 - security of, 57, 59, 336n47
 - security problems in Tom-Skype, 179, 318n24
- Slammer worm, 159, 234
- Smart devices, 249, 324n114
 - appliances and, 128
 - cell phones and, 99, 164
 - computers as, 40
 - credit card readers and, 172–173
- Smart networks, 3, 6, 56, 189
- Smith v. Maryland*, 79–80, 99
- SMS. *See* Texting
- Sneak peeks, 194
- Sniff packets, 53, 85, 160, 178–179, 199
- Snow, Brian, xv, 39
- Social networks, 56, 138, 191, 248
- Software as a Service (SaaS), 126
- Software Defined Networks (SDNs), 239
- Source code, 33, 173
- South Africa, 207, 301n2
- Soviet Union, xi–xii, 19, 59, 98, 179, 275n83, 277n21
 - Ames and, 98, 163–164
 - atomic bomb and, 8
 - Black Friday and, 135
 - Cold War and, 8, 17, 113–114, 128, 135, 148, 151, 201, 213, 215
 - embassy tunnel and, 163
 - evolving communication technologies and, 128, 135, 302n46
 - Glen Cove site and, 148
 - Hanssen and, 163, 165
 - industrialization of, 213
 - intruder identification and, 147–148, 151, 162–163, 165–166, 307n43
 - KGB and, 147, 162, 165
 - Lourdes, Cuba site and, 148
 - Mutually Assured Destruction and, 215
 - Philby and, 162–163
 - policy issues and, 213, 215
 - Sputnik and, 19
 - spying and, 147–148, 151
- Spam, 39, 54, 145–146
- Special Powers Act, 206
- Specter, Arlen, 105
- Speed-dial, 13
- Sperry Rand, 147
- Spoofing, 52–55, 58, 60–61, 113, 187, 196
- Sports Illustrated, 34
- Sproull, Lee, 33
- Sputnik, 19
- Spying, xii, 9, 184, 187, 235, 249, 278n27

- alternative information sources and, 147
- Ames and, 162–164
- attacks by nation-states and, 165–171
- bribery and, 151, 152
- business communications and, 147–152
- China and, 166–171
- Cold War and, 147–148, 151
- defense contractors and, 148
- ECHELON and, 152
- economic, 147–153, 165–171
- effectiveness of, 98, 119
- evolving communication technologies and, 133, 135
- faxes and, 151
- Glen Cove site and, 148
- Hanssen and, 163, 165
- HUMINT and, 151
- insider attacks and, 162–165
- intruder identification and, 146–153, 161–171
- KGB and, 147, 162, 165
- legal issues and, 68, 75, 89, 92–94
- limitation of CALEA and, 246–248
- Lourdes, Cuba site and, 148
- microwave transmissions and, 147–148
- military assets and, 146
- Min and, 163
- Philby and, 162–163
- Titan Rain and, 167, 170
- trash analysis and, 151
- Trojan-horse programs and, 166–167, 170
- Spyware, 133, 168
- Stealth technologies, 150
- Stengart v. Loving Care Agency*, 298n122
- Strategic Defense Initiative (“Star Wars”), 150
- Streaming video, 131–132, 334n20
- Subpoenas, 79, 94, 99, 102, 192–193, 204–205, 305n86, 337n63
- Suez War, 135, 215
- Suite B algorithms, 47
- Sun Microsystems, xi, 155–156, 189, 191, 272n38, 304n70, 309nn72,73
- Supercomputers, 21, 38, 117, 124–125, 264n42
- Supervisory control and data acquisition (SCADA) systems, 158, 180–181, 239
- Supply chains, 154–157, 197
- Surveillance, xii, 34–35, 256
 - anonymity tools and, 139–141
 - behavioral, 97, 252
 - bugs and, 9, 69–70, 104, 106, 197, 249
 - business communications and, 147–152
 - Communications Assistance for Law Enforcement Act (CALEA) and, 2–3, 82–85, 88, 119, 177, 186–190, 196, 200, 219, 223, 233, 240, 245–250
 - court orders and, 71, 79–81, 84, 89–90, 99–104, 136, 177, 184, 186
 - data mining and, 97, 136, 191, 252
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - Digital Telephony proposal and, 81
 - economic, 147–153
 - Einstein projects and, 120–122, 219, 233
 - exigent letters and, 193–195, 205, 207, 256
 - FISA and, 65 (*see also* Foreign Intelligence Surveillance Act (FISA))
 - fishing expeditions and, 75
 - hot numbers and, 194
 - immigrants and, 209–212
 - interception capacity and, 82
 - international telegrams and, 175
 - intruder identification and, 146, 152, 163, 167–168
 - lasers and, 249, 337n53
 - Martus and, 217–218

- microwave transmissions and, 147–148
- minimization requirement and, 74
- modern issues of, 7–12
- Murphy's law and, 195–198
- Omnibus Crime Control and Safe Streets Act and, 65, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
- peering points and, 53, 89–90
- pen registers and, 79–86, 89, 99–104, 133, 137, 187, 190, 194, 196, 219, 248, 285n120, 292n31, 337n63
- police state and, 73
- policy recommendations for, 233–236, 240, 243–244, 247–252
- postal service and, 66, 157, 186
- President's Surveillance Program (PSP) and, 90–95, 112, 200, 243, 252, 256, 286n137, 338n3
- probable cause and, 11, 74, 77–78, 157, 337n63
- Protect America Act (PAA) and, 2, 93, 207, 240, 327n20, 336n41
- public network traffic and, 119–122
- radio waves and, 69, 133
- Regulation of Investigatory Powers Act (RIPA) and, 327n21
- right policy stance for, 250–253
- risk of excessive, 209–215
- search warrants and, 2–3, 66, 70 (*see also* Search warrants)
- sneak peeks and, 194
- traffic analysis and, 133–139
- transactional information and, 59–60, 72, 99–101, 103 (*see also* Transactional information)
- Triggerfish and, 103, 248
- USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- Vietnam War protests and, 68, 73, 175
- watchlists and, 175
- wiretaps and, 2–3, 65 (*see also* Wiretaps)
- Sweden, 49, 94
- SWIFT database, 111–112, 160
- Switzerland, 114, 141
- Syracuse University, 108
- Taiwan, 150, 154, 167–168, 169
- Targeted advertising, 103–104
- Tash Hepting et al. v. AT&T Corporation et al.*, 92–93, 176
- Taxol, 150
- TCC, 114
- TCP/IP (Transmission Control Protocol/Internet Protocol)
 - best-effort basis and, 24
 - communication network architectures and, 20, 23–25, 264nn50,51
 - evolving communication technologies and, 132–133
 - handshakes and, 40–41, 53, 132
 - reliability and, 24–25, 38–42
 - security issues and, 37–42, 46, 53, 56, 269n3
 - virtual private networks and, 46, 119, 179, 233, 336n47
- Teamster's Union, 69
- Telecom Italia, 164
- Telecommunications Act, 89, 181
- Telecommunications Workers Union, 55
- Telegraphs, 1, 7, 213
 - effect of, 123
 - fast U.S. adoption of, 212
 - privacy and, 175, 212
 - relationship with railroad networks and, 13–14
 - wiretaps and, 66
- Telemarketing, 59, 104
- Telephones, 11, 259n31
 - area codes and, 14, 16, 194
 - Bell and, 7, 13, 19
 - call forwarding and, 29, 72, 81
 - call length and, 134

- Telephones (cont.)
- cell phones, 1, 3–4, 7 (*see also* Cell phones)
 - CDRs and, 89 (*see also* Call Detail Records (CDRs))
 - central office and, 16–17, 27–28, 71, 178, 182, 184–186, 199, 226–227, 248
 - common carriers and, 284n110, 301n30
 - communication during crises and, 226–227
 - communication network architectures and, 13–18, 21, 26–31, 261nn2,3, 262nn19,29, 263n37
 - convergence with computers, 128–130
 - Digital Telephony proposal and, 81
 - dumb terminals and, 4, 6
 - E911 and, 129
 - effectiveness of surveillance and, 99–103, 113–115, 119, 292n31
 - Electronic Communications Privacy Act (ECPA) and, 80, 84, 99, 192–194
 - Europol and, 136–137
 - evolving communication technologies and, 123, 128–132, 135–137, 301n30
 - exigent letters and, 193–195, 205, 207, 256
 - FCC and, 5, 84–85, 128, 132, 219, 227, 229, 243–245, 258n20, 259n21, 269n101, 283n103, 284n112, 300n18, 302n40
 - 4ESS switch and, 72, 181
 - frames and, 71–72
 - friendly circuits and, 71
 - Gamma Guppy intercepts and, 135
 - hot numbers and, 194
 - intruder identification and, 172, 312n115
 - iPhones and, 4, 6–7, 33, 99, 127, 134, 230
 - legal issues and, 66–71, 78–89, 92–93, 279n45, 284n110
 - local exchange and, 14, 16, 78
 - local loop and, 71–72, 81–82
 - location tracking and, 3, 7, 14, 16, 107, 129–130, 178, 182–185, 197
 - long-distance calls and, 4, 39–40, 82, 88, 236, 279n45
 - Mobile Switching Center and, 129, 183, 248
 - modern networks and, 78–85
 - network convergence and, 180–182
 - network development of, 13–17
 - number of annual calls on, 30
 - out-of-band signaling and, 29, 40
 - PANS (Pretty Advanced Network Services) and, 4
 - phone cards and, 7, 72, 98
 - policy risks and, 205, 213, 220, 249
 - post-cut-through dialed digits and, 82, 84
 - POTS (plain old telephone service) and, 4
 - Prohibition Era and, 259n31
 - PSTN, 4–6 (*see also* Public Switched Telephone Network (PSTN))
 - reliability of, 16–17
 - repeaters and, 16, 230
 - satellite, 107, 228
 - security and, 39–42, 58–59, 177, 179, 184, 186–188, 191–202
 - signaling systems and, 4–5, 29, 39, 79–80, 180–181, 265n62, 266n71
 - sneak peeks and, 194
 - speed-dial and, 13
 - traffic analysis and, 133–138, 176
 - trap-and-trace devices and, 80, 82, 86, 89, 99, 102–103, 285n120, 292n31
 - TSD 3600 and, 114
 - VoIP and, 4 (*see also* Voice over Internet Protocol (VoIP))
 - Television, 31, 32, 226
 - Telex, 123
 - Tenth Amendment, 200
 - Terrorists

- Al-Qaeda and, 2, 88, 94, 98, 107–112, 161, 208, 210, 284n117
- anthrax and, 222
- Authorization for Use of Military Force (AUMF) and, 93
- communication technologies and, 136, 138
- context of, 222–223
- cyberattacks and, 8–9, 95, 145–146, 153, 168, 171, 208, 235–236, 333n7
- cyberwar advantages of, 171
- DDoS attacks and, 161
- defining, 8, 294n69
- domestic, 208–209
- German saboteurs and, 208, 222
- Hamas and, 109
- Hezbollah and, 109
- identifying, 208–210
- immigrants and, 209–212
- indoctrination and, 209
- investigation of, 210–212
- Islamic fundamentalists and, 209–210
- jihadists and, 109, 209–211
- Ku Klux Klan and, 208
- McVeigh and, 209
- natural disasters and, 223
- New York Police Department (NYPD) and, 209–211
- preradicalization and, 209
- prosecution rates and, 294n69
- public cooperation and, 211–212
- radicalization process and, 209–210
- resources of, 165, 317n9
- right policy for, 233, 241, 246–247, 256
- self-identification and, 209
- September 11 attacks and, xi, 2, 85–86 (*see also* September 11 attacks)
- slow CIA response to, 284n117
- urban riots and, 208
- USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- wiretaps and, 75, 77, 85, 91, 93–94, 98–100, 107–112, 119, 181, 184, 191–194, 203, 207–212, 218, 222–226, 281n71, 282n77, 286n137
- Terrorist Surveillance Program, 94, 286n137
- Texas Instruments, 149
- Texting, 7, 28–30, 72, 121, 319n39
- asynchrony of, 29–30
- for business, 29
- China and, 29–30
- communication network architectures and, 265n61, 266nn70,71
- data on voice networks and, 28–30
- denial of service and, 182
- evolving communication technologies and, 131–132
- excessive collections risks and, 190
- Japan and, 29
- limitations of, 30
- network convergence and, 180–182
- politics and, 29–30
- popularity of, 29
- reliability of, 30
- security risk of, 178–179
- store-and-forward architecture and, 180
- 32-bit address space, 20, 62
- ThorpeGlen, 137
- Tibet, 167–168
- Tice, Russell, 94
- Tien, Lee, 116
- Titan Rain, 167
- Title III order
- excessive collection risks and, 192
- legal issues and, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
- President's Surveillance Program (PSP) and, 90
- Tom-Skype, 179
- Top-level domains, 49, 62, 142
- Tor (The onion routing), 139–141, 275n84

- Torvalds, Linus, 33, 268n94
- Toshiba, 154
- Tradenet, 266n68
- Traffic analysis
- AT&T and, 176–177
 - Computer and Internet Protocol Address Verifier (CIPAV) and, 133
 - evolving communication technologies and, 134–139
 - first-responder communications and, 230
 - Narus machines and, 176
 - National Security Agency (NSA) and, 176–177
 - use in criminal investigations and, 99–102
- Transactional information, 260n49
- anonymization tools and, 139–141, 191, 222, 321n64
 - business communications and, 147–152
 - Call Detail Records (CDRs) and, 89, 99, 102, 136, 192–194, 200, 207, 220, 240, 248
 - court orders and, 101–103
 - critical infrastructure risks and, 157–161
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - Europol and, 136–137
 - evolving communication technologies and, 129, 136–139
 - excessive collection risks and, 102–103, 189–195
 - legal issues and, 72, 78, 89
 - limitation of CALEA and, 246–248
 - location and, 98, 99–104
 - Martus and, 217–218
 - National Security Letter (NSL) and, 99–100, 103, 139, 192–194, 322n85
 - pen registers and, 99–104
 - policy risks and, 205, 222
 - private company access and, 103–104
 - real-time access and, 79, 89, 99–102
 - security and, 59–60, 160, 177–179, 182–183, 190–191, 199–200, 241–242, 248
 - SWIFT database and, 111–112
 - Tom-Skype and, 179
 - traffic analysis and, 133–139
 - value in investigations and, 98, 99–101
 - wiretaps and, 72, 78, 82, 89, 98–99, 112, 121, 177–179, 182–183, 190–191, 199–200, 205, 222
- Transactional Records Clearinghouse (TRAC), 108–110
- Trap-and-trace devices, 80, 82, 86, 89, 99, 102–103, 285n120, 292n31
- Traynor, Patrick, 180
- Treverton, Gregory, 216–217
- Triacetone triperoxide (TATP), 111
- Triggerfish, 103, 248
- Trojan horses, 54, 94, 146, 166–167, 170
- Truman, Harry, 69
- Trust anchor, 61–62
- Truth and Reconciliation Commission, 207
- TSA, xii
- Tsunamis, 223, 267n85
- Tutelage, 219
- Twentieth Century Fox, 34
- Twitter, 134
- Two-party consent, 71
- Uniformed Sanitation Men v. Commission of Sanitation*, 105
- United Kingdom, 5, 49, 66, 258n16
- Bloody Sunday and, 206–207
 - communication network architectures and, 17–18, 261n12, 266n71
 - effectiveness of wiretapping and, 98, 110
 - evolving communication technologies and, 131, 138, 141

- intruder identification and, 152, 163, 170, 172
- policy risks and, 203, 211, 215, 235, 242, 326n12, 327n21
- Regulation of Investigatory Powers Act (RIPA) and, 327n21
- United Nations, 62, 208, 217
- United States, xi–xii
- Alien and Sedition Acts and, 256
- Bill of Rights and, 1, 10, 67, 189–190
- copyright and, 218
- Cold War and, 8, 17, 113–114, 128, 135, 148, 151, 201, 213, 215
- critical infrastructure risks and, 157–161
- DARPA and, 19, 39, 47, 62, 123–124, 127, 141, 233, 238, 334n20
- Data Encryption Standard (DES) and, 44–45, 47, 114–115, 244, 257n4
- economic espionage against, 146–153
- embassy security and, 216–217
- export control and, 116–119
- Federal Communications Act and, 67–70, 284n110
- Fifth Amendment and, 11, 67
- First Amendment and, 10, 78, 175–176, 192, 204, 218, 252, 316n3, 337n62
- FISA and, 65 (*see also* Foreign Intelligence Surveillance Act (FISA))
- Fourth Amendment and, 11, 66–67, 70, 73, 75, 79, 90–92, 99, 127, 189–190, 205, 250
- George H.W. Bush and, 81
- George W. Bush and, 88, 90–97, 108, 111, 120, 176, 203–204, 207–208, 286n137, 336n41
- immigrants and, 209–212
- lowering economy of, 255
- as moral leader, 203
- Mutually Assured Destruction and, 215
- National Infrastructure Protection Plan and, 157
- Omnibus Crime Control and Safe Streets Act and, 65, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
- organized crime and, 8–9, 66, 72–73, 97, 106, 130, 164, 172, 312n111
- phone usage data of, 30
- President's Surveillance Program (PSP) and, 90–95, 112, 200, 243, 252, 256, 286n137, 338n3
- Prohibition Era and, 66–68, 73, 259n31
- Protect America Act (PAA) and, 2, 93, 207, 240, 327n20, 336n41
- Radio Act and, 67
- search warrants and, 66, 70, 79–80, 133, 207, 260n47, 279n47
- Sputnik and, 19
- Telecommunications Act and, 89, 181
- Tenth Amendment and, 200
- USA PATRIOT Act and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- value of communications security and, 215–219
- wiretap policy of, 9–10 (*see also* Wiretaps)
- writs of assistance and, 189–190
- United States Pacific Command, 217
- United States v. Miller*, 79
- United States v. Poeta*, 105
- United States v. United States District Court for the Eastern District of Michigan et al.*, 75
- Universal Declaration of Human Rights, 203
- University of California, 242
- University of Toronto, 167, 179
- USA PATRIOT Act
- legal issues and, 77–78, 86, 90, 99–100, 157, 203, 207, 223, 279n47
- National Security Letter (NSL) and, 99–100
- policy risks and, 203

- USA PATRIOT Act (cont.)
 President's Surveillance Program (PSP)
 and, 90
 rule of law and, 207
- U.S. Army Information Systems
 Engineering Command, 166
- U.S. Army Space and Strategic Defense,
 166–171
- USA Today*, 2, 88, 93, 176
- USB sticks, 158, 164
- U.S. Bureau of Export Administration,
 116
- U.S. Civil War, 66, 256
- U.S. Constitution, 250
 European Convention on Human
 Rights and, 203
 Fifth Amendment, 11, 67
 First Amendment, 10, 78, 175–176,
 192, 204, 218, 252, 316n3, 337n62
 Fourth Amendment, 11, 66–67, 70,
 73, 75, 79, 90–92, 99, 127, 189–190,
 205, 250
 Preamble of, 200–201
 technical obsolescence and, 202
 Tenth Amendment, 200
 Universal Declaration of Human
 Rights and, 203
- U.S. Court of Appeals, 2
- U.S. Cyber Command, 333n7
- U.S. Department of Agriculture, 147
- U.S. Department of Defense, 6, 19, 119,
 140, 338n3
 Chinese attacks and, 166
 economic espionage and, 153
 intruder identification and, 150, 153,
 169, 171
 legal issues and, 286nn137,142
 right policy stance for, 239, 245
- U.S. Department of Energy (DoE), 21,
 159
- U.S. Department of Homeland Security
 (DHS), 120–122,
 231, 244, 245
- U.S. Department of Justice (DoJ). *See*
also Federal Bureau of Investigation
 anti-terrorism bill and, 85
 Communications Assistance for Law
 Enforcement Act (CALEA)
 compliance and, 188–189
 defining terrorism and, 108
 effectiveness of wiretapping and, 102,
 108, 112, 120
 Einstein projects and, 120–121
 fishing expeditions and, 75
 legal issues and, 68, 75, 90–92,
 277n21, 280n56
 National Security Division and, 108
 Office of Intelligence Policy and
 Review (OIPR) and, 90
 pen registers and, 101–102
 policy risks of wiretapping and, 205,
 208
 President's Surveillance Program (PSP)
 and, 90–92
 security risks of wiretapping and, 188,
 194
 rule of law and, 208
 wiretapping the press and, 205
- U.S. Department of State, 218
- United States v. United States District
 Court for the Eastern District of
 Michigan et al.*, 75
- U.S. Department of the Treasury, 245
- USENET, 21
- Usernames, 58, 169, 179, 196–197,
 324n111
- U.S. General Accounting Office, 81
- U.S. Immigration and Naturalization
 Service, 109
- U.S. Marshals Service, 100–101
- U.S. MASINT (Measurement and
 Signals Intelligence), 163
- U.S. National Academies of Science and
 Engineering, 97
- U.S. National Telecommunications and
 Information Administration, 142

- U.S. Navy, 39, 109, 140, 173
- U.S. Supreme Court, 11
- Brandeis and, 67, 312n115
- email privacy and, 298n122
- evolving communication technologies and, 127
- illegal search and seizure and, 67
- “interception and divulgence” ruling and, 175
- Jackson and, 201–202
- policy risks and, 204
- Preamble of Constitution and, 200–201
- security risks and, 175, 200–201, 325n130, 337n62
- wiretaps and, 66–70, 75, 77, 79, 92, 121, 288n158
- U.S. Term Limits, Inc., v. Thornton*, 200
- U.S. Undersea Warfare Center, 173
- Valachi, Joseph, 73
- Varian, Hal, 242
- VeriSign, 62
- Verizon, 88, 103, 132, 198, 226, 227, 266n71
- Vernam, Gilbert, 44
- Vetrov, Vladimir, 165
- Victimless crimes, 73, 104
- Vietnam War, 68, 73, 135–136, 175, 198, 255
- Virtual private networks (VPNs), 46, 119, 179, 233, 336n47
- Viruses
- host attacks and, 53–55
- Melissa, 54, 274n64
- security challenges against, 39, 53–55, 57, 124, 133, 145–146, 168, 197, 274n63, 274n64
- self-replication and, 53–54
- Trojan horses and, 54, 94, 146, 166–167, 170
- Visitor Location Register (VLR), 26–27
- Vodafone Greece, 177, 185, 234–235, 240–241
- Voice over Internet Protocol (VoIP), 3, 7, 27–28
- communication during crises and, 227–228
- communication network architectures and, 20, 27–28, 31
- Communications Assistance for Law Enforcement Act (CALEA) and, 84–85, 188
- deep packet inspection (DPI) and, 132, 219–220
- design principles and, 41–42
- E911 and, 85
- Ethane and, 238–239
- evolving communication technologies and, 128–129, 132, 137, 143
- FBI and, 84–85
- FCC and, 84–85
- functionality during crises and, 228
- legal issues and, 2, 84–85, 284n112
- location and, 85, 137, 182–185
- network convergence and, 181
- policy risks and, 219–223
- routing of, 27–28
- security issues and, 42, 179–188, 200, 238, 244–246, 318n26, 334n20
- Skype and, 4, 6, 28, 57, 59, 119, 179, 222, 232, 260n33, 336n47
- telephone/computer convergence and, 128, 128–130
- Vonage, 228
- Walker, Vaughn, 94
- Wall Street Journal*, 85, 161
- Wal-Mart, 128, 154, 259n29
- Warhol, Andy, 31
- Warren, Samuel, 10, 260n43
- Washington Post*, 76, 205, 219, 220
- Washington sniper, 103, 291n19
- Watchlists, 175

- Watergate scandal, 69, 76, 175, 204, 249
- WhoIs, 143
- Wikipedia, 32, 142, 143
- Windows Live, 142
- Wiretap Report*, 74, 78, 104–107
- Wiretaps, xii–xiii
 - accountability and, 73
 - analyzing fielded communication products and, 113–117
 - Athens Affair and, 177, 187, 234–235, 240–241
 - black-bag jobs and, 71, 133
 - built-in security and, 198–200
 - Carnivore and, 85, 187, 196, 243, 245
 - CDRs and, 89 (*see also* Call Detail Records (CDRs))
 - Church Committee and, 60, 69, 77, 175
 - Cisco architecture risks and, 196–197
 - Communications Assistance for Law Enforcement Act (CALEA) and, 2–3, 82–85, 88, 119, 177, 186–190, 196, 200, 219, 223, 233, 240, 245–250, 284nn110,114, 292n31, 297n113, 320n48
 - Computer and Internet Protocol Address Verifier (CIPAV) and, 133, 245, 249
 - consensual overhear and, 71, 106
 - convictions from, 81–82
 - current law and, 242–243
 - deep packet inspection (DPI) and, 130–133, 219–222, 234–235, 240–241
 - ease of installation, 6
 - effectiveness of, 97–122
 - Electronic Communications Privacy Act (ECPA) and, 80, 84, 99, 192–194
 - expense of, 74
 - FBI and, 68–69 (*see also* Federal Bureau of Investigation (FBI))
 - Federal Communications Act and, 67
 - fishing expeditions and, 75
 - FISA and, 65 (*see also* Foreign Intelligence Surveillance Act (FISA))
 - 4ESS switch and, 72, 181
 - Fourth Amendment and, 66–67, 70, 73, 75, 79, 90–92
 - frames and, 71–72
 - friendly circuits and, 71
 - government's need for, 2
 - Hoover and, 68, 72–73, 95, 277n19, 278nn26,27
 - illegal search and seizure and, 67–68
 - “interception and divulgence” ruling and, 175
 - interception capacity and, 82
 - journalists and, 68–69, 76–77, 94, 164, 204–208, 217, 337nn62,63
 - King and, 69
 - legal issues of, 65–95, 204–206
 - local loops and, 71–72, 81–82
 - location tracking and, 3, 7 (*see also* Location tracking)
 - loop extenders and, 71
 - methods for, 71–72
 - minimization requirement and, 74
 - modern networks and, 78–85
 - narcotics investigations and, 97–98
 - national security cases and, 65–77, 87, 91–93, 97–99, 103–108, 111, 120, 122, 175, 194, 208, 215–218, 223
 - Olmstead and, 11, 70
 - Omnibus Crime Control and Safe Streets Act and, 65, 73–78, 84, 90, 100–107, 189, 192, 248, 280n52, 292n31
 - peering points and, 53, 89–90
 - pen registers and, 79–86, 89, 99–104, 133, 137, 187, 190, 194, 196, 219, 248, 285n120, 292n31, 337n63
 - policy risks from, 203–223
 - post-cut-through dialed digits and, 82, 84
 - post-September 11, 85–87

- President's Surveillance Program (PSP)
 and, 90–95, 112, 200, 243, 252, 256,
 286n137, 338n3
 probable cause and, 11, 74, 77–78,
 157, 337n63
 Prohibition Era and, 66–68
 Protect America Act (PAA) and, 2, 93,
 207, 240, 327n20, 336n41
 Radio Act and, 67
 radio waves and, 71 (*see also* Radio)
 remote delivery risks and, 187–188
 results for criminal cases, 104–107
 right policy stance for, 250–253
 roving, 80–81, 86, 130, 172
 security risks from, 175–202
 suspect's knowledge of, 73
 technical solutions to, 240–241
 Telecommunications Act and, 89, 181
 telegraph and, 66
 terrorists and, 75, 77, 85 (*see also*
 Terrorists)
 Title III order and, 73–78, 84, 90,
 100–107, 189, 192, 248, 280n52,
 292n31
 transactional information and, 72, 78,
 82, 89 (*see also* Transactional
 information)
 trap-and-trace devices and, 80, 82, 86,
 89, 99, 102–103, 285n120, 292n31
 two-party consent and, 71
 USA PATRIOT Act and, 77–78, 86, 90,
 99–100, 157, 203, 207, 223, 279n47
 U.S. Department of Justice (DoJ) and,
 68, 90–92, 102, 108, 112, 120, 188,
 194, 205, 208, 277n21
 U.S. Supreme Court and, 66–70, 75,
 77, 79, 92, 121
 warrantless, 2–3, 67–78, 87–95,
 175–176, 187, 192, 203–204, 207, 212,
 223, 240, 243, 246, 252, 336n41, 338n3
 Watergate scandal and, 69, 76, 175,
 204, 249
 workings of, 71–72
 Woolsey, James, 152–153
 World Trade Center, 222, 226, 228–229
 World War I era, 43, 134, 208, 213,
 270n17
 World War II era, 255–256, 278n27
 civil liberty curtailments during, 201
 Enigma and, 44
 German crypto system and, 44
 Hoover authorization and, 68
 housing shortage of, 202
 Japanese crypto system and, 107, 135
 Navajo code talkers and, 45
 supply-chain complexity and, 154
 terrorists' revenge for, 223
 World Wide Web Consortium (W3C),
 141
 Worms, 234, 273n44
 host attacks and, 53–55
 Morris, 47–48, 54, 145
 self-replication and, 53
 Slammer, 159, 234
 Trojan horses and, 54, 94, 146,
 166–167, 170
 Wright, Lawrence, 94
 Writs of assistance, 189–190
 Xxx nameserver, 142
 Y2K issue, 158
 Yahoo!, 87, 121, 142, 298n122
 Yamamoto, Isoroku, 107
 Yoo, John, 90
Youngstown Sheet & Tube Co. v. Sawyer,
 90
 YouTube, 31, 55, 142
 Yuen Foong Paper company, 150
 Yurchenko, Vitaly, 162
 Zazi, Najibullah, 111, 295n86
 Zittrain, Jonathan, 56
 Zombies, 53, 145–146, 234, 305n2,
 333n7
 Zones, 49, 51, 61, 142, 273nn47,51