
Index

- 911 databases, 370, 373
- A5 cryptoalgorithm, 259
- AMD, 262
- AOL (America Online), 55
- AT&T
 - CCIS protection by, 354, 356
 - cooperation with NSA, 303
 - secure phones made by, 233
- Abernathy, Ralph, 161
 - FBI letter about, 362
- Abuse of power, 170–171
- Addresses for messages, 100
- Adleman, Len, 69–80, 229
- Administrative Office of the US
 - Courts, *See* US Courts,
 - Administrative Office of
- Admissibility of wiretap evidence, 372
- Advanced Encryption Standard (AES), 30, 31
 - adoption of as FIPS 197 (2001), 30, 250, 251, 279, 317
 - Pentagon approval of, 279
- Advanced Telephony Unit, 215, 368, 390
- Agency for International Development
 - opposition to EES, 377
- Agnew, Spiro, 362
- Air Force Cambridge Research Center (AFCRC), 64–65
- Air Force and IFF equipment, 65
- Air Force Office of Warfighting
 - Integration, 115
- Air travel, identification in, 136
- Airborne intelligence collection, 98
- Aircraft Sabotage Act, 138
- Aircraft identification devices, 64–65
- Al Hadaf, 167
- al-Qaeda, 90, 309, 310, 331
- al-Zahawiri, Ayman, 331
- Albatross machine, 106
- algebraic techniques, 31
- Albee, Edward, 157
- Alternate Encryption Technique, 344
- Amazon, 264, 274
- American Airlines, 274
- American Bar Association, 210
- American Civil Liberties Union,
 - 362–363
 - v.* NSA, et al., 302
- American Communist Party, 159
- American Council on Education study
 - panel, 71, 260
 - v.* FCC, 295
- American Express, 153
- American Library Association, 166
- American National Standards Institute, X3T1, 347
- Ames, Aldrich, 91, 130, 289, 391
 - secret searches and, 318–319
 - wiretaps on, 391
- Amplitude modulation, ciphertext contamination in, 45

- Analog scramblers. *See* Voice scramblers
- Ancient World
identification in, 357, 378
- Angola, surveillance in, 226
- Anonymity, 271,
- Anonymizer.com, 272
- Anti-ballistic missile treaty, 349
- Anti-drug efforts, 137–138
military involvement in, 138
wiretapping in, 209–210
- Antiterrorist and Effective Death Penalty Act, 374
- Anti-war movement
FBI surveillance of, 363–364
- Anti-war protests, 161–162, 165, 320
- Anti-Wiretap Statute, 177
- Appel, Edward, 245
- Applied Cryptography* (Schneier), 121–122, 250, 315
- Arbaugh, William, 263
- Argentina
Use of DES by, 345
- Argos intelligence satellites, 350
- Armed Forces Communications Electronics Association (AFCEA), 353
- Arms Export Control Act, 120–121
- Arvad, Inga, 184
- Ashcroft, John, 284
- Asiacrypt conference, 352
- Asymmetric cryptosystems, 38
- Atomic Energy Act, 390
- Attacks
avoiding on US network, 118
differential power analysis, 46
on US military computer networks, 115
resistance to described as security, 30
SHARK algorithm succumbed to, 31
- Attestation, 263
- Audio recordings, 3
- Authentication, 390
- Authenticity, 12, 37–38
in banking, 47
importance, compared with privacy, 341
meaning of, 338
in public-key cryptography, 39–41, 316
- Authorization, 37
- Automated Information Systems
sensitive information on, 346
- Automatic teller machines, 66
- Autonomy, right to, 142
- Acxiom, 155
- Back doors, 7, 206, 234–241
- Baker, Stewart, 245, 283
- Balanced Budget and Emergency Deficit Act, 346
- Baldwin, Hanson, 363
- Ballistic missile testing, 94
- Bandwidth, 55
- Bank of America, 274
- Bank of Credit and Commerce International, 138
- Banking Security Standards Committee, 29
- Banking
cryptographic needs in, 47–48, 73–76
NSDD-145 opposed by, 75
use of cryptography by, 357
- Barbara, Joseph, 191
- Batiste, Narseal, 310
- Battle of Jutland, 352–353
- Beecher, William, 197
- Bell Labs, 353
- Berlekamp-Massey Algorithm, 352
- Bernstein, Daniel, 255
- Bhang metre, 349
- Biddle, Francis, 180
- Biden, Joseph, 231
- bin Laden, Usama, 306, 383, 388
- Birth Control Act, 150–151
- Black, Hugo, 158
- Block ciphers, 30
- Blossom, Eric, 390

- Bollinger, Lee, 378
- Bombe cryptanalytic machine, 352
- Bootlegging era, 148–149, 177–179
- Bork, Robert, 153, 361
- Born secret doctrine, 390
- Boston, wiretapping in, 187
- Botnet, 119
- Boyce, Christopher, 350
- Brafman, Benjamin, 368
- Brandeis, Louis
 - on privacy, 148, 149
 - on wiretaps, 147–150
- Brandon, Henry, 164
- Britain
 - Clipper program in, 244–245, 378
 - cryptologic connection with US, 378
 - economic espionage by, 49
 - key-escrow program in, 244
 - mail privacy, 145
 - police force established in, 128
 - policy on cryptography, 279
 - privacy, legal hostility to, 378
 - public key cryptography in, 344
 - Regulation of Investigatory Powers Act, 279
 - surveillance in, 145, 224–225
 - wiretapping in, 342
- British intelligence
 - hampered by DES, 345
- British wiretap law, 342
- Brokat Informationssysteme, 379
- Brooks, Clinton, 78, 83, 205, 231, 348
- Brooks, Jack, 346
 - and Digital Signature Standard, 80
 - and NSDD-145, 75
 - standards acts authored by, 66, 76–77
 - computer security act authored by, 76–77
- Brown, Hank, 138
- Brownell, Herbert, 369–370
 - privacy policy clarified by, 188
 - wiretapping supported by, 182–183
- Bugs, 175, 371
 - court decisions on, 188–189
 - vs. wiretapping, 130, 188–189
- Burns, Conrad, 247
- Business
 - adoption of cryptography by, 52–53
 - Clipper chip opposed by, 7–8, 236–238
 - cryptographic needs of, 47–52
 - dependence on Internet, 55
 - export controls and, 8
 - future of cryptography in, 56
 - industrial espionage and, 314
 - public-key cryptography in, 316
- CALEA, 220–224, 319, 320, 370
 - applied to VoIP, 270, 294–301
 - capacity requirements of, 373
 - funding of, 319–320
 - limits on, 373
 - transactional data in, 373
- CAVE cipher, 22
- Cable TV records, privacy of, 154
- Caesar Cipher, 339
- California
 - electronic surveillance in, 348
 - wiretapping in, 187
- Call detail reporting, 303
- Call logging, 133
- Call signs, 100, 352
- Call tracing, 358, 373. *See also* Caller-ID
- Callender, James Thomas, 145
- Caller-ID, 358, 372, 392
 - kidnapping cases, use in, 370
 - and wiretaps, 392
- Cambodia bombing, wiretapping
 - abuses after, 163, 197
- Campbell, William, 193
- Capitol Hill
 - communications from, 353
- Capstone chip, 239, 350, 377
- Caracristi, Ann, 243
- Carnegie-Mellon University, 262
- Carnivore, 269, 270, 382, 383, 292.

- See also* Digital Collection Service 1000 (DCS)
- CAST-256 algorithm, 379
- Castro, Fidel
CIA interest in, 349
- Celebrities
surveillance of, 362–363
- Cellular telephones, 2, 6, 22, 55, 203, 206, 299, 325
cloned, detection of, 392
lack of privacy of, 377
- Censorship in Civil War, 146
- Census Bureau, 156–157, 170, 361
- Census data
access to, 361
- Central Intelligence Act, 63
- Central Intelligence Agency, 63, 391
and drug war, 348
and ECHELON, 255
Foreign Broadcast Information Service of, 348
and U2 spy plane, 349
- Central facilities in key production, 32, 38
- Certicom, 252
- Certificates in public-key cryptography, 40–41, 258
- Chalabi, Ahmad, 107
- Challenge and response in public-key cryptography, 41
- Charney, Scott, 245, 372
- Chaum, David, 272
- Chennault, Anna, 196
- Chicago, wiretapping in, 187
- China
cyberwarfare, 115, 116
economic espionage by, 49
as emerging world power, 266, 304, 328
development of cryptosystems, 304
surveillance in, 226
- ChoicePoint, 155
- Chosen plaintext, 339
acquisition of, 339
- Chosen-plaintext assumption, 27
- Church Committee on privacy, 137, 170, 156, 201–202
- Cipher machines, 19
- Ciphers, 13, 21, 24–27
- Ciphertext
exploitation of, 102
plaintext contamination of, 45
- Ciphertext-only attacks, 26
- Cisco, 274
- Citicorp, 47, 341–342
- Civil War
telegraph in, 146
wiretapping in, 177
- Civil rights movement, 184
- Civiletti, Benjamin, 243
- Clark, Ramsey
on organized crime, 192
on wiretapping, 187, 192
wiretapping permission refused by, 161
- Clark, Thomas, 181–182, 361
- Classified Information Procedures Act, 140
- Cleartext, 13
- Clinton, William J., 281, 348
Escrowed Encryption Standard supported by, 234
and Intelligence Authorization Act, 139
wiretapping for terrorism supported by, 223
- Clinton, Hillary, 216
- Clipper chip, 350. *See also* Escrowed Encryption Standard
authorization to purchase, 377
development of, 377
device unique key of, 377
digital telephony proposal and, 375
vulnerabilities of, 377
- Clipper program, 232, 234–236. *See also* Escrowed Encryption Standard
business objections to, 7–8, 48, 236–238
controversy over, 236–239

- in Escrowed Encryption Standard, 234–236
- OECD support for, 245–246
- revisions to, 240–241
- Cobra Ball intelligence aircraft, 349–350
- Code
 - meaning of, 338
- Code division multiplexing, 351–352
- Code groups, 14
- Codebooks, 33
- Codebreakers, The* (Kahn), 63, 66, 90, 353
- Codes, 13–14
 - one-part, 338
- Cold War, 62–63, 123, 280, 324, 328
- Collateral intelligence, 96, 352
- Colombia, surveillance in, 226
- Colossus cryptanalytic machine, 355
- Combination surveillances, 371
- Combiners, 339
- Command and Control, 134, 377
 - nuclear, 343
 - public key cryptography in, 343
- Commercial Comsec Endorsement Program (CCEP), 72–73, 345
 - modeled on ITP, 345
- Committee in Solidarity with the People of El Salvador (CISPES), 166–167
- Committee on Government Operations, 346
- Committee on National Security Systems (CNSS), 251
 - Policy Number 15, 251
- Common Channel Interoffice Signaling
 - protection of, 354, 356
- Common-channel signaling, 110
- Communications Assistance for Law Enforcement Act (CALEA), 220–224, 319–320
 - capabilities sought, 222–223, 223–225
 - connections with encryption, 227
 - cordless phone protection, 176
 - Federal Bureau of Investigation sought, 205–206, 219–221, 389
 - funding for, 221, 223
 - international extension sought, 224–225
 - precursor as Digital Telephony Proposal, 205–207
- Communication security monitoring, 47
- “Communication Theory of Secrecy Systems, The” (Shannon), 63
- Communications bandwidth, 265
 - division of responsibility in, 391
- Communications cover, 44
- Communications deception, 355–356
 - imitative, 355–356
 - manipulative, 355–356
- Communications in police work, 133–137
- Communications intelligence (COMINT), 93–95
 - budget, as fraction of total intelligence budget, 337
 - encryption impact on, 110–112
 - impediments to, 108–110
 - prospects for, 322–323
 - secrecy in, 103–104
 - status of, 104–107
 - success of, 353
 - taxonomy of, 95–103
 - value of, 350–351
- Communication Security (COMSEC)
 - Security failure analyses in, 45
 - equipment, tamper resistance of, 46
- COMSEC materials control system, 33
- COMSEC monitoring, 47
- Communist Party of the US
 - threat of, 183–184, 362
- CompuServe, 55
- Computer Professionals for Social Responsibility, 206
- Computer Security Act, 231
 - cost of, 346
 - enactment of, 76–77
 - NSA response to, 77–78

- Computer System Security and Privacy Advisory Board, 376
- Computer intelligence, 114–117
- Computer standards, 66, 76–77
- COMSEC. *See* Communication Security
- Conference calls, 132
- Confusion, in information theory, 31
- Congress and cryptography, 246–248, 319
- Congressional communications
 - security of, 353
- Congressional members, wiretapping of, 185–186
- Consensual overhear, 129, 211
- Constitutional protection from wiretapping, 176
- Consular facilities, intelligence gathering by, 90, 118
- Content Scrambling System (CSS), 259
- Convictions from wiretapping, 212–216
- Coplon, Judith, 182
- Copying machine, 51
- Corcoran, Thomas, 158
- Cordless and cellular telephones, 2, 6, 22, 176, 206
- Cordless telephones, 351–352
- Counterintelligence, 53
- Court orders for wiretapping, 194, 198–199
- Cotter, Don, 329
- Covert communication, 44, 338
- Credentials, 36–37, 40
- Credit cards
 - as privacy threat, 153
 - for tracking, 136
- Cribs in ciphertext-only attacks, 26
- Crime, technological advances in, 136
- Criminal investigation
 - textbooks of, 392
- Crook, Colin, 378
- Croswell, Edgar, 191
- Cryptanalysis, 102
 - differential, 31, 250
 - by intercept equipment, 391
 - as a production activity, 352
 - linear, 31, 250
 - responsibility for, 391
 - of WWII cryptosystems, 352
- Crypto '81, 390
- Crypto conference, 352
- Cryptograms, 258
- Cryptographic Devices
 - Ladner, 356
 - KG-84, 356–357
- Cryptographic Equipment
 - NSA control over, 345
- Cryptographic equipment
 - Type I, 345
 - Type II, 345
- Cryptographic keys
 - editions of, 340
 - sale of, 340
- Cryptographic systems
 - classification of, 338
 - secrecy of, 338
- Cryptography, 2, 11–14, 315–318
 - for anonymity in transactions, 4
 - back doors in, 7
 - business adoption of, 52–53, 259
 - business needs for, 47–52
 - busts in, 45
 - Capstone chip in, 239
 - Clipper chip in, *See* Clipper program
 - commercial future of, 56
 - Congressional reaction to, 246–248
 - computing cost of, 390
 - consumer products, 259
 - differential power analysis and, 46
 - dynamic key distribution in, 34–35
 - elliptic-curve, 252
 - elliptic-curve (Diffie-Hellman), 254
 - Escrowed Encryption Standard for, 234–236
 - export controls and, 8, 256
 - government opposition to, 6–9, 54, 69–72
 - history of, 19–26
 - Internet effect on, 54

- key management in, 32–34
- large-scale, 17–19
- lifetime of systems, 29–30
- market for, 6, 337
- message digest function and, 252
- most common, 355
- mechanization of, 57–60
- Multi-level Information Systems Security Initiative for, 242
- national encryption policy for, 231–232
- National Research Council report on, 242–244
- and OECD, 245–246
- one-time systems, 16
- packet communication and, 41
- Pretty Good Privacy, 229–230
- for privacy, 323
- privacy invasion on, 170
- public-key, 38–41, 68–69
- publications about, 343
- quantum computing and, 28
- rate of progress in, 390
- secure communications in, 46–47
- security in, 43–44
- Skype and, 111,
- small-scale, 14–17
- standards in, 53
- strengths and weaknesses of, 26–27, 35–38
- supporting technologies in, 45–46
- in telephony, 232–234
- theories of, 339
- unbreakable, 105
- utility of, 350, 355
- workfactors in, 27–29
- Cryptologic Research Unit, 245
- CRYPTON algorithm, 379
- Cryptosystems
 - lifetimes of, 340, 353
- Cuba
 - CIA interest in, 349
- Cuban missile crisis, 103
- Culture dependence in privacy, 143
- Currency transfers, 47
- DEAL algorithm, 379
- DFC algorithm, 379
- DMS-100 telephone switches, 132
- Dam, Kenneth, 242
- Damm, Arvid Gerhard, 58
- Dartmouth College, 270
- Dash, Samuel, 187
- Data Encryption Standard (DES), 9, 24–25, 30, 31, 250, 344, 345, 391
- development of, 67
- exporting, 121
- limitations of, 29
- NSA attempt to kill, 346
- replacement needed for, 249
- replaced by AES, 31, 30
- TSD 3600 in, 233–234
- triple-DES, 29
- Data mining, 291–292
- Data retention, 291–292, 294
 - in combat of child pornography, 294
- Data Retrieval System, 169
- Databases, 153–154, 331
 - matching of, 361
- Databrokers, 155
- David Snow, 340
- Davida, George, 70
- Davis, Ruth, 344
- deCSS, 260
- Defections, 324
- Defense Advanced Research Projects Agency (DARPA), 273
- Defense Authorization Act, 138
- Defense Support Program (DSP)
 - satellites, 92
- de Marenches, Henri, 49
- Democracy, privacy for, 143, 170
- Demodulating modem signals, 101–102, 354
- Denmark, encryption policy in, 245
- Denial of service, distributed, 119
- Depth in Vigenère systems, 22
- Detection of interception, 52
- Deterrence in crime prevention, 127–128
- Diagnosis

- of cryptosystems, 111
- of signals, 101–102
- Dicks, Norman D., 248
- Differential power analysis, 46
- Diffie, Whitfield, 68–69, 108, 354, 356, 372, 377, 390
- Diffie-Hellman key exchange, 40–41, 252, 315
 - for business, 315
 - development of, 69
 - elliptic curve, 254
 - in Key Exchange Algorithm, 239
 - in TSD 3600, 238
- Diffusion, in information theory, 31
- Digital Collection Service 1000 (DCS), 269
- Digital Content Protection LLC, 262
- Digital Millennium Copyright Act (DMCA), 260
- Digital Rights Management, 48, 259
- Digital signal processing, 391
 - in secure telephones, 376
- Digital Signature Algorithm, 239
- Digital Signature Standard, 80–83, 254
 - speed of, 347
- Digital signatures, 39, 49, 69, 80–83, 340–341
 - primitive, 340–341
- Digital Telephony Proposal, 205–206.
 - See also* CALEA
 - Clipper chip and, 375
 - costs of, 368
 - FBI support for, 218–219, 389
 - and kidnapping cases, 389
 - revised, 219–224
 - and transactional information, 216
 - wiretapping value asserted in, 207
- Digital telephone switches, 132
- Direct standard alphabets in Vigenère systems, 21
- Direction finding, 352
- Disinformation, 113, 356
- Distribution of keys, 33–35
- Dobrynin, Anatoly, 106
- Domestic organizations, privacy violations against, 159, 162, 166–167
- Domestic security, wiretapping for, 181, 195–198
- Domestic terrorism, wiretapping targeting of, 211, 391
- Dominican Republic sugar case, 195
- Double DES. *See* triple DES
- Double Vigenère systems, 22
- Douglas, William O., 158
- Downgrading schedule for classified information, 339
- Dragging key, 352
- Drug Enforcement Agency, 372
- Drug trafficking
 - military involvement against, 138
 - wiretapping targeting of, 210–211
- Drugs
 - market inelasticity of, 369
 - as a national security issue, 348
 - reducing consumption of, 369
- Dual-use items, 121
- DVD Content Control Association, 260
- DVDs, 259
- Dynamic key distribution, 34–35
- Dynamic routing, 109, 354
- E2 algorithm, 379
- eBay, 54, 264, 274
- ECHELON, 50, 255
- eLoan, 274
- E-mail, cryptography for, 229–230
- Eastland, James, 160
- Eavesdropping
 - meaning of, 173
 - punishment of, 144
- Economic espionage, 49–50
- Editions of code books, 340
- Editions of cryptographic keys, 33, 340
- Egypt, 350
- Ehrlichman, John

- burglary authorized by, 197
- wiretapping by, 164
- El Salvador, surveillance in, 225
- Electromagnetic pulse, 355
- Electromagnetic shielding, 45
- Electronic Banking
 - penetrations of, 341–342
- Electronic Cash, 342
- Electronic Commerce, 342
 - definition of, 342
- Electronic Communications Privacy Act, 203
- Electronic Data Interchange (EDI), 342
- Electronic code books, 24
- Electronic Frontier Foundation (EFF), 261
- Electronic funds transfers, 47 357
- Electronic intelligence (ELINT), 94
- Electronic surveillance, 129–137, 175, 372, 375. *See also* Wiretapping
 - in California, 348
 - in New York State, 348
 - for political purposes, 337
 - in Watergate, 337, 358
- ElGamal, Tahir, 81
- Ellsberg, Daniel, 197
- Else, George, 181
- Email
 - abuse of, 119
 - escrow of, 378
 - and Internet addresses, 268. *See also* Simple Mail Transfer Protocol
 - Skipjack declassified for protecting on military networks, 25
 - ubiquitous, 55
- Embassies, intelligence gathering by, 90, 98
- Emergency wiretap orders, 372
- Emissions intelligence (EMINT), 94
- Emitter Identification, 94, 352
 - commercial uses of, 392
- Employee supervision, 326
- Encrypted Communications Privacy Act, 246
- Encrypted messages. *See also* Cryptography
 - automatic recording of, 101
 - and wiretapping, 227
- Encrypted traffic
 - vulnerability of, 377
 - wiretapping and, 390
- End-to-end keying, 44
- Engelman, Carl, 343
- England. *See* Britain
- English common law
 - knock and announce, 318
- Enigma machine, 58
- Entertainment industry, 48, 260
- Envelopes, 12
- Equifax credit bureau, 153
- Escrow agents
 - security clearances of, 378
- Escrowed encryption. *See* Key escrow
- Escrowed Encryption Standard (EES), 9, 7, 232, 234–236. *See also* Clipper chip
 - agencies opposed to, 377
 - authorization to purchase, 377
 - call for comments on, 377
 - Clipper chip revisions in, 240–241
 - controversy over, 236–239
 - vulnerabilities of, 377
- ESS series telephone switches, 132
- Eurocrypt conference, 352
- European Commission,
 - protections on electronic communications, 293
- European communications, use of encryption, 256
- European Convention on Human Rights
 - wiretapping and, 374–375
- European Council, interception supported by, 225
- European Court
 - wiretapping, rulings on, 374–375
- European Parliament, 255
- European Union, interception supported by, 224–225

- European Union
 - wiretapping and, 375
- Evidence from wiretapping, 179–188
- Exploitation process, 102
- Export Administration Act, 120–121
- Export Control, 8, 120–123, 232, 256, 354, 379
 - and Escrowed Encryption Standard, 240
 - foreign availability in, 356
 - of high-grade systems, 356–357
 - impact on domestic use of cryptography, 378
 - NRC recommendations against, 242
- Export control office
 - real function of, 357
 - organizational position of, 357
- Eyraud, Charles, 343
- EZPass, 292

- FROG algorithm, 379
- Face-to-face interaction, 1
- Fair Credit Reporting Act, 153
- Falconview, 116
- Falklands War, 345
- Farber, Dave, 263
- Federal Bureau of Investigation (FBI)
 - 168, 208, 215
 - Abernathy, opinion of, 362
 - Advanced Telephony Unit of, 368
 - Anti-war movement and, 161–162
 - Anti-war movement, surveillance of, 363–364
 - CISPES investigated by, 166–167
 - criticized by FISA Court, 282
 - Damages paid to SWP by, 362
 - DoJ criticism of, 391
 - Digital Telephony Proposal supported by, 219–224, 389
 - European Union and, 375,
 - journalists bugged by, 163–165
 - Library Awareness Program, 165–166
 - mail openings, 159
 - and Martin Luther King, Jr., 159–161
 - and NSA, 83–85
 - political investigations by, 158, 161–163
 - Socialist Workers Party and, 159
 - Socialist Workers Party harassment of, 362
 - threat of communist party as seen by, 362
 - wiretapping by, *See* Wiretapping
 - “wiretapping” Internet, 269
- Federal Communications Act, 150, 178–179, 183, 188
- Federal Communications Commission,
 - Federal Information Processing Standards
 - and Clipper chip, 234, 240
 - establishment of, 66
 - origin and importance of, 343–344
 - Advanced Encryption Standard, 279
 - Federal Information Security Management Act (FISMA), 289
- Federal Privacy Act, 154
- Federal procurement, 377
- Federal Register*, 249
- Federal Standards
 - exceptions to, 377
- Feige, Fiat, Shamir system, 344–345
- Feige, Uriel, 344–345
- Feistel, Horst, 64–67, 343, 344
- Felten, Ed, 261
- Felten v. RIAA*, 261, 262
- Ferguson, Niels, 261, 262
- Fiat, Amos, 344–345
- Fifth Amendment, 144
- Financial transactions
 - reporting of, 341
- Fingerprinting, 126, 135
- Fingerprints
 - functions of in police work, 357
- FIPS. *See* Federal Information Processing Standards
- Firefly cryptography method, 74
- Firewalls, 119

- First Amendment, 144, 150–151, 255, 261
- First-responders, 254
- Fishing trawlers, 97
- Fixed position cellular telephony, 325
- Fleet Broadcast System, 33
- Flying Saucers, 349
- Ford, Gerald, 143, 348
- Foreign Broadcast Information Service, 348
- Foreign Intelligence Surveillance Act (FISA), 140, 202–203, 280, 286, 288, 301, 319
- Foreign Intelligence Surveillance Court, 202, 282, 289
 - and secret searches, 318–319
- Forensics, 126
- Forfeiture laws, 357
- Forrest, John Waterhouse, 198
- Fort Meade
 - NSA buildings at, 353
- Fortezza cards, 238, 239, 242
 - SECRET traffic, use for, 377
- Fortier, Michael, 368–369
- Foster, James, 293
- Foster, Vincent, 216, 372
- Fourteenth Amendment, 144, 361
- Fourth Amendment, 4, 144, 149, 152, 176, 318, 330
- France
 - court control of investigations in, 392
 - economic espionage by, 49
 - mail, 148
 - surveillance by, 145
- Franklin, Benjamin, 145
- Free Haven project, 273
- Freeh, Louis, 327, 328, 369–370, 373, 375, 378
 - Digital Telephony Proposal sought by, 219–220
 - encryption restrictions sought by, 227, 247–248
- Frequency division multiplexing, 351–352
- Frequency modulation, ciphertext contamination in, 46
- Frequency-hopping radios, 44
 - used to deliver products, 337
- Friedman, William Frederick, 58–59
- Frost, Mike, 98
- Fuller, Samuel, 378
- Funding, 71–72
- Future Secure Data System, 242
- Gaming, online, 55, 56, 305
- Gambling as wiretapping target, 209, 213–214
- Gamma Guppy intelligence operation, 350–351
- Gelb, Leslie, 378
- General Accounting Office, 364
- General cryptographic systems, 13
- General cryptographic system as public information, 338
- General Motors, 341
- General Telephone and Electronics (GTE), 376
- Germany
 - economic espionage by, 50
 - encryption policy in, 246
- Gingrich, Newton
 - cellular telephone overheard, 377
- Girardin, Ray, 193
- Gonzalez, Alberto, 294
- Google, 55, 264, 265, 305
- Gore, Albert, 256
- Government Information Security Reform Act (GISRA), 289
- Gleason, Andrew, 343
- Glickman, Daniel, 80
- Global Cryptography, conference on, 376
- GNU Emacs pseudo-random number generator, 338–339
- Goldman v. United States* case, 188
- Goldwasser, Shafi, 343
- Golitsin, Anatoli, 391
- Goodlatte, Bob, 247

- Goss, Porter J., 248
 Gotti, John, 130, 311, 391
 Government Communications
 Headquarters (GCHQ), 106
 public key cryptography at, 344
 Government. *See also* Federal Bureau
 of Investigation (FBI)
 cryptography opposed by, 6–9, 54,
 69–72
 data collection by, 154
 economic espionage by, 49–50
 policies and programs of, 120
 wiretapping by, *See* Wiretapping
 “Government’s Classification of
 Private Ideas, The” (report), 346
 Graham, Ronald, 378
 Gramm-Rudman-Hollings Act, 78
 Grassley, Charles, 282, 284, 388
 Gravano, Sammy, 130
 Great Britain. *See* Britain
 Greece, surveillance in, 226
 Gregg, Judd, 279, 290
Griswold v. Connecticut case,
 150–151, 319
 Gubitchev, Valentin, 182
 Gulf War, 113, 355
 operational intelligence during,
 348–349
 computer viruses in, 356
- HIPAA. *See* Health Insurance
 Portability and Accountability Act
 Haldeman, H. R., 197
 Hall, Marshall, 343
 Halperin, Morton, 197–198
 Harris, Jo Ann, 390
 Hart-Rudman report, 306
 Hash algorithms, 251, 254
 Hasty Pudding Cipher, 379
 Health-care industry, 48
 Health Insurance Portability and
 Accountability Act (HIPAA), 48
 Hebern, Edward, 58–59
 Hellman, Martin, 68–69, 81, 378
 Helsing, Cheryl, 75
- Hemingway, Ernest, 349
Hepting, et al. v. AT&T Corp. et al.
 case, 303
 Hersh, Seymour, 107, 277
 High Bandwidth Digital Content
 Protection (HDCCP), 261, 262
 High-definition television (HDTV),
 262
 High energy microwave, 355
 High-Speed Anti-radiation Missile,
 355
 Hogan, Doug, 344
 Hogan, Frank, 348
 Holloway, Jack, 356
 Home Box Office, 355
 Hong Kong, 116, 226
 Hoover, J. Edgar, 369–370. *See also*
 Federal Bureau of Investigation
 journalists bugged by, 363
 and Martin Luther King, Jr., 160
 on organized crime, 190–192
 Hops for messages, 100
 Hot-potato routing, 109
 Hotmail, 274
 House Judiciary Committee, 372
 Human intelligence (HUMINT), 89,
 323
 Hurley, Deborah, 379
 Huston, Tom, 165
- IBM2984 banking system, 67
 Identification cards, 136
 Identification Friend or Foe (IFF)
 devices, 64
 Identification, technology for, 135–136
 Identity, 271
 Identities
 absolute vs. consistent, 390
 Identity provider, 274
 Identity theft, 52, 119
 Iglehart, Dick, 212, 370
 Imitative communications deception,
 355–356
 Improvements in telecommunications
 impact on crime of, 370

- Incriminating conversations
 - overheard in wiretapping, 368
- India,
 - nuclear tests by, 103
- Indonesia, surveillance in, 226
- Industrial espionage, 341, 342
 - foreign, 342
 - by governments, 49–50
- Industrial Tempest Program
 - CCEP modeled on, 345
- Infiltration, 129
- Informants, 143, 161, 360, 362
- Information theory, 356
- Information warfare, 112–114, 116–117
- Infrared imaging, 135, 137
- Infrastructure, *See* Trusted Platform Technology. *See also* Public-Key Infrastructure
- Inman, Bobby Ray, 71, 260, 344, 353
- Instant messaging, 55
- Insurrections and wiretapping, 195
- ISDN. *See* Integrated Services Digital Network (ISDN)
- Integrated Services Digital Network (ISDN), 110
 - secure telephones for, 354–355
- Integrity of messages, 12
- Intel Corporation, 261, 262
- Intellectual property, 5, 123, 259
- Intelligence Authorization Act, 139
- Intelligence collection
 - embarrassments in, 349
- Intelligence
 - communications, *See* Communications intelligence (COMINT)
 - prospects for, 322–326
 - security from, 117–119
 - spectrum of, 88–93
 - from wiretapping, 179–187
- Intercept equipment
 - capabilities of, 357
 - cryptanalysis in, 391
- Interception
 - in communications intelligence, 95–103
 - impediments to, 108–110
 - national policies on, 224–226
 - one-sided, 351
 - signal processing problems of, 354
 - technology, development of, 9
- Interdiction of crimes, 127
- Internal Revenue Service, 169
 - browsing of citizen files by, 364
- International Business Machines, 343–344
 - telephone security of, 342
- Alternate Encryption Technique of, 344
- 2984 system of, 67
- Lucifer cryptographic system of, 67, 344
- Secrecy orders against, 344
- International Covenant on Human Rights, 142, 360
- International Standards Organization
 - consideration of DES as standard, 347
- International Traffic in Arms Regulations, 70
- International support
 - for Clipper chip, 244–246
 - for wiretapping, 224–225
- International terrorism, US
 - jurisdiction over, 138
- Internationalization,
- Internet, 54, 118, 327
- Internet cafes, 56
- Internet Engineering Task Force (IETF) 299
- Internet Protocol, 42, 267, 268
 - version 6, 268
- Internet Protocol Security Protocol (IPSec), 43
- Intrusion detection systems, 119
- Investigations, police, 126–127
- Irvine v. California* case, 188
- Isa, Tina, 373, 389
- Islamic fundamentalism,

- threat of terrorism, 307, 308
- Israel, 350
 - attack on *USS Liberty*, 351
 - investigating terrorism in, 307
- Jackson, Robert, 179–180
- Jamming, 355
- Japan,
 - cyberattacks on, 115
 - economic espionage by, 49
- Japanese-American relocation plan, 156, 170, 320, 361
- Jefferson, Thomas, 145
- Jeffery, Seymour, 344
- Johansen, Jon Lech, 260
- Johnson Island, 355
- Johnson, Lyndon
 - King wiretapped by, 160
 - political intelligence for, 163
 - wiretapping abuses by, 195
 - wiretapping opposed by, 163, 186, 193, 363
- Jones, R. V., 60–61
- Judicial review
 - immunity from, 374
- Judicial tolerance
 - of secret searches, 318–319
- Jumpseat satellites, 99, 107
- Juniper algorithm, 254

- KG-84, 356–357
- KI-23, 350
- KL-7 rotor machine, 29
- Kahn, David, 63, 66
- Kallstrom, James, 84, 348
 - on cellular telephones, 222
 - wiretapping capabilities sought by, 223, 391
- Kamchatka Peninsula air defense system, 349–350
- Kammer, Raymond, 78–81, 83–84, 205, 231, 347, 348
- Karn, Philip, 121
- Katrina, Hurricane, 267, 312
- Katz, Charles, 151, 319, 330, 331
 - Charles Katz v. United States* case, 151, 189, 330
- Katz, Julius, 378
- Katzenbach, Nicholas
 - on wiretapping for national security, 183, 363
 - wiretapping limitations imposed by, 180, 186
- Kennedy, Joan, 164
- Kennedy, John F., 343
 - cryptosystems for nuclear control systems ordered by, 64
 - wiretapping abuses by, 163, 195
 - wiretapping of, 184
- Kennedy, Robert
 - and organized crime, 190–191
 - wiretapping abuses by, 160, 196
- Kennedy, Ted, 164
- Kerckhoffs principle, 338
- Kerrey, Bob, 247
- Kerry, John, 138
- Key agreement, 341, 344. *See also* Key exchange
- Key distribution, 33–35. *See also* Key management
 - bottlenecks in, 340
 - dynamic, 34–35
 - in public-key cryptography, 39–40
- Key Distribution Center (KDC), 340. *See also* Key Management Facility
- Key escrow, 7, 9, 25, 227, 233–241, 257. *See also* Key recovery
 - in DoD, 378
 - of Type I keys, 377
- Key exchange, 341, 344
- Key Exchange Algorithm (KEA), 239
- Key management, 32–34, 376. *See also* Key distribution
 - as vehicle for escrow, 378
- Key management facilities (KMFs), 34–35, 340
- Key negotiation 341, 344. *See* Key exchange
- Key recovery. *See also* Key escrow

- in DoD, 378
- Keys, 13
 - in large-scale cryptography, 17–18
 - management of, 32–34
 - recovery of, 7, 241
- Kidnapping cases, 211, 389
 - 911 databases in, 370
 - caller-ID use in, 370
 - other crimes and, 391
 - use of wiretaps in, 370, 391
 - utility of wiretaps in, 370
- King, Martin Luther, Jr., 159–162
 - advisors of wiretapped, 364
 - FBI reports on, 362
 - wiretapping of, 362
- Kissinger, Henry
 - negotiation strategy discussed with Dobrynin by, 106
 - wiretapping abuses by, 163, 197
- Knock and announce doctrine, 318
- Known-plaintext attacks, 26
- Koblitz, Neal 252 379
- Kocher, Paul, 46
- Kolender, Chief of Police of San Diego, et al. v. Lawson* case, 136
- Kollar-Kotelly, Colleen, 282
- Kopelev, Lev, 354
- Korean Airlines (KAL) 007, 349–350, 351
- Kraft, Joseph, 163–164, 363
- Krasnoyarsk radar, 349
- Kravitz, David, 81
- Krypton cards, 242
- Kyllo v. United States*, 152, 319

- L.A. 8, 167, 168, 308, 320
- Lacrosse satellites, 91
- Ladner, 356
- Lamarr, Hedy, 344
- Landau, Susan, 290, 291, 347, 348, 379
- Large-scale cryptography, 17–19
- Latham, Donald, 75
- Law Enforcement Access Field (LEAF)
 - in EES, 235–237, 376
- Law Enforcement Exploitation Field (LEEF), 376. *See also* Law Enforcement Access Field
- Law enforcement, 96, 318
 - covert operations services and, 139
 - electronic surveillance in, 133–137, 273
 - foreign intelligence and, 139
 - foreign powers and, 139
 - vs. national security, 137–139
 - police origins in, 127–128
 - prospects for, 318
 - solution vs. prevention in, 125–127
 - wiretapping in, *See* Wiretapping
- Leahy, Patrick, 246, 282, 284, 285
- Leibler, Richard, 344–345
- Lenstra, Arjen, 252
- Letter opening, meaning of, 173
- Levi, Edward, 363
- Levison, Stanley, 159
- Lexis-Nexis information broker, 153
- Liberty*, 97, 351
- Liberty Alliance, 274
- Librarians, privacy protected by, 165–166
- Library Awareness Program, 165, 364
- Lifetimes of cryptosystems, 29–30, 340, 340
- Linear shift register, 352
- Link keying, 43
- Link layer, 42
- Links for messages, 100
- Linux, 260, 263
- Lloyds Bank, 66
- Local loop, 296
- Lockheed Martin
 - secure phones made by, 354–355, 376
- Locks, 13
- LOKI97 algorithm, 379
- Long, Edward, 185–186
- Long-term keys, 35
- Lookup tables, (as confusion in information theory), 31, 250
- Lord, William, 115

- Lorenz SZ40 cryptographic machine, 355
- Los Angeles 8. *See* L.A. 8
- Los Angeles Office of Public Defender, 212
- Lotus Company, 153
- Lourdes Cuba intercept station, 351
- Low-orbit satellites, 99
- Lucifer cryptographic systems, 67, 344
- Lyons, John, 82
- M-134a rotor machine, 59
- MARS algorithm, 250, 379
- MCI, 153
- MD5 algorithm, 253
- MIT Press, 230
- MMORPG. *See* Massively multiplayer on-line role playing games
- MQV elliptic-curve algorithm, 254
- Magenta algorithm, 379
- Magnetometry, 136
- Maher, David, 233
- mail cover
by NSA, 391
- Mail delivery
privacy in, 145, 144–146, 148
security of, 11–12
- Mailsafe program, 229
- Malone, James, 374–375
- Manferdelli, John, 381
- Manipulative communications
deception, 355–356
- Marfino
cryptographic laboratory at, 354
- Markup languages,
Hypertext Markup Language (HTML), 266
Standard Generalized Markup Language (SGML), 266
Extensible Markup Language (XML), 266
- Marion, Pierre, 49
- Mark X IFF system, 64, 343
- Mark XII IFF, 343
Mode 4 of, 343
- Markey, Hedy Keisler, 344
- Martin, William, 353
- Mask files for computer chips, 338
- Mass market software, 357
- Massachusetts Institute of Technology, 270
- Massachusetts, wiretapping in, 187
- Moussaoui, Zacarias, 310
- Massively multiplayer on-line role playing games, 55, 305
- Material objects, examination of, 136
- Mathematics
relation to cryptography, 343
theory behind tables in DES, 30
- Mayfly algorithm, 254
- McCain, John, 247
- McCarran-Walter Act, 168
- McCarthy, John, 69, 168
- McCord, James, 358
- McGrath, J. Howard, 180
- McLane, James, 163
- McNulty, Lynn, 81, 82, 347
- McVeigh, Timothy, 209, 306, 310, 368–369
- Mead Data Central, 74
- Measurement and signatures
intelligence (MASINT), 92
- “Meet in the middle” attack, 340
- Menezes, 254
- Merkle, Ralph, 68
- Message digest function, 252, 253
- Message digests, 340–341
- Message indicators, 343
- Methods in codebreaking, 102
- Meyer, J. A., 69–70
- Micali, Silvio, 343, 378
- Microphone surveillances, 372
in Gotti case, 358
in Stanfa case, 373, 311
secret “searches” to plant, 318–319
- Microsoft Corporation, 262, 274, 381
Passport, 274
Windows, 263
- Microwave communications, 96

- Military Cooperation with Civilian Law Enforcement Agencies Act, 138
- Military aircraft
IFF used by, 343
- Military
in law enforcement, 138
cryptography dominated by, 315
real-time intelligence for, 113
response of to public use of cryptography, 316
- Miller, Mitchell, 151–152
- Miller, Victor, 252, 379
- Mills, W. H., 343
- Minimization in wiretapping, 217
- Missile testing, 94
- Mitchell, Bernan, 353
- Mitchell, John, 163–165
- Mitnik, Kevin, 350
- Mitre Corporation, 343
- Mobility in communications, 6, 36
- Modem signals
demodulating, 101–102
interception of, 109
speed of, 354
- Mogul project, 349
- Moles, 391
- Molniya communication satellites, 99
- Monoliteral substitution in cryptography, 19
- Moore's law, 339
- Morris, Robert, 353
- Motorola
secure phones made by, 354–355
- Multi-level Information Systems Security Initiative (MISSI), 242
- Multinational corporations
use of cryptography by, 357
- Multiple Vigenère systems, 22
- Multiplexed messages, 100, 351–352
- Munitions, 121
- Muskie, Edward, 197
- Mykotronx, 350
- NAACP v. Alabama* case, 150–151, 319
- NSA. *See* National Security Agency (NSA)
- NIPRNet. *See* US Department of Defense
- NSDD-145. *See* National Security Decision Directive 145
- Nardone, Frank Carmine, 150, 178–179
- Nardone v. United States* case, 150, 179
- National Association for the Advancement of Colored People (NAACP), 150–151
- National Bureau of Standards. *See also* National Institute of Standards and Technology (NIST)
failure to support DES as international standard, 347
meetings at, 340
NSA influence on, 347
- National Command Authority, 343
- National Computer Security Center, 353
- National Crime Information Center, 134, 169
- National Guard, 138
- National Institute of Standards and Technology (NIST). *See also* National Bureau of Standards (NBS) and Computer Security Act, 76–78
Computer Security Division (CSD), 291
for computer standards, 66, 76–84
and DES standard, 29, 249
digital signature and, 80–81
Escrowed Encryption Standard required by, 237
NSA and, 78–85
NSA influence on, 347
as possible standards developer, 346
reimbursable funds of, 346
- National Research Council, cryptography panel

- report of, 242–244
- clearances of, 378
- members of, 378
- and public cryptography, 390
- National Science Foundation (NSF), 71
- National security,
 - cyberwarfare and, 115
 - export controls and, 8
 - identification cards and, 136
 - Iran and, 107
 - Iraq and, 107
- National Security Agency (NSA), 318, 345, 376
 - and Computer Security Act, 76–83
 - COMINT product, 353
 - legal control of cryptographic publication thwarted, 260
 - creation of, 63
 - Cryptographic Algorithms as NATO standards, 344
 - current programs of, 301
 - deal with Software Publishers Association, 357
 - and DES standard, 67, 249
 - and Digital Signature Standard, 82
 - and FBI, 83–85
 - and Indian nuclear tests, 102
 - IBM, assistance to, 342
 - licensing Certicom technology, 252
 - Michael Hayden and, 277
 - vs. NIST, 317
 - payment of royalties by, 345
 - as possible standards developer, 346
 - property owned by, 353
 - public-key cryptography opposed by, 70
 - relations with Congress, 346
 - reservations about public debate, 376
 - Howard Rosenblum at, 344
 - Suite B, 254
 - telegram privacy violations by, 158, 391
 - Type I and Type II equipment, 345
- National Security Decision Directive 145 (NSDD-145), 74–76
- National security, 6
 - communications intelligence in, 93–103
 - concept of, 87–88
 - cyberwarfare and, 115
 - drugs and, 348
 - education and, 348
 - intelligence spectrum in, 88–93
 - vs. law enforcement, 137–139
 - signals intelligence in, 93–95
 - perceived need for heightened by attacks, 90
- Naval Research Laboratory, 273
- Nessen, Ronald, 222
- Net keying, 43
- Network Address Translation, 267, 268
- Network layer, 42
- Neumann, Peter, 378
- Neutron activation analysis, 136
- “New Directions in Cryptography” (Diffie and Hellman), 69
- New York State
 - electronic surveillance in, 348
 - wiretapping in, 187
- Newspapers,
 - mailing of, 145
 - weblogs and search engines replacing, 51
- Nicolai, Carl, 70
- Nigeria, surveillance in, 226
- Ninth Amendment, 144
- NIST. *See* National Institute of Standards and Technology
- Nixon, Richard, 348
 - resignation of, 200, 337
 - wiretapping abuses by, 163–165, 196–198
- NOFORN classification, 344
- No lone zone, 340
- Nokia, 274
- Nonlinear shift registers, 24
- Norman, Lloyd, 363

- Normandy invasion, 355
 communications deception in, 355–356
 communications intelligence in, 350–351
 NATO, 254, 356–357
 North Korea
 capture of *USS Pueblo*, 349
 Northern Ireland,
 investigating terrorism in, 307
 Norway Seismic Array (NORSAR), 92
 Nuclear Command and Control, 343
 Nuclear Regulatory Commission
 opposition to EES, 377
 Nuclear explosions
 detection of, 349
 Nuclear magnetic resonance, 136
 Nuclear weapons
 arming of, 343

 Odom, William
 on NSA leadership, 75–76
 on NSDD-145, 76
 Office of Naval Research, 273
 Oil industry, 48
 use of cryptography by, 357
 Oklahoma City Bombing, 306, 310, 368–369
 Olmstead, Roy, 148–149, 178
Olmstead v. United States case, 178–179
 Omnibus Crime Control and Safe Streets Act, 192–195, 318, 318, 372,
 Omnibus Diplomatic Security and Antiterrorism Act, 138
 One-part code, 338
 Onion routing, 273
 Open-source intelligence, 89
 Open-source software, 267
 Operations intelligence, 89, 348–349
 Optical fiber, 108, 264, 354
 Order of battle, 95
 Organization for Economic Cooperation and Development (OECD), 245–246
 members of, 378
 privacy recommendations, 379
 Organized crime
 visibility of, 190–192
 wiretapping of, 189–192, 193
 Oshima, Baron, 350–351
 Oxygen absorption band, 337–338
 Outsourcing, 265
 Ozzie, Raymond, 378

 PCMCIA cards, 238–239, 242
 Packet communication, 41
 Packet sniffer, 269
 Palestinian Students, General Union of, 169
 Passivity in communications intelligence, 114
 Passwords
 one-time, 341–342
 Patent secrecy orders, 344–345
 NSA assistance with removing, 344–345
 US Army request for, 344–345
 value of to industry, 344
 Patents, 347–348
 for rotor machines, 58–59
 secrecy orders for, 70, 344
 Pay-tv scrambling, 355
 Peace organizations, privacy violations against, 157
 Pearl Harbor, 90, 280
 Peele, Robert, 128
 Pelton, Ronald, 351
 Pen registers, 133, 203, 358, 373
 Penkofsky, Oleg, 91
 Pentagon
 approval of Advanced Encryption Standard, 279
 operational intelligence at, 348–349
 “Pentagon Papers” (Ellsberg), 197
 Periods in Vigenère systems, 22
 Permissive Action Links, 343
 public key cryptography in, 343

- Permutations, 31
- Personal Digital Assistants, 55
- Pers Z organization, 106
- Philby, Kim, 353–354
- Phishing, 52, 119
- Photographic intelligence (PHOTINT), 91–92
- Physical layer, 42
- Physical protection, 12, 36
- Plaintext, 13, 45
 - chosen, 339
 - recognition of, 338, 339
- Plamondon, Lawrence, 198
- Poindexter, John, 74–76, 346
- Poindexter directive, 74–76
- Polar orbit communication satellites, 99
- Police Cooperation Working Group, 225
- Police. *See also* Law enforcement courts, 357–358
 - first wiretapping by, 177
 - history of, 127–128
 - influence on law making, 358
 - modern investigative techniques, 359
- Political discourse, privacy for, 143
- Popular Front for the Liberation of Palestine (PLFP), 167
- Pollard, Jonathan, 91
- Polly Klaas murder
 - lack of wiretapping in, 369–370
- Polyalphabetic encryption, 21
- Polynomials, 250
- Portable devices, 50, 54
- Posse Comitatus Act, 137, 360
- Postal Act of 1792, 145
- Postal delivery systems
 - privacy in, 144–145, 157–158
 - security of, 11–12
- Pressler, Larry, 327
- Pretty Good Privacy (PGP) program, 229–230
- Prevention and Punishment of Hostage-Taking Act, 138
- Prevention of crimes, 127
- Primitive Digital Signatures, 340–341
- Princeton University, 261
- Privacy, 360. *See also* Wiretapping
 - in 1940s, 156–158
 - in 1950s, 159
 - in 1960s, 159–165
 - in 1970s and 1980s, 165–167
 - in 1990s, 169
 - in American society, 143
 - Brandeis on, 148, 149
 - Church Committee on, 137, 170, 170, 200–202
 - in conversations, 11
 - dimensions of, 141–142
 - in early years, 144–148
 - and Fourth Amendment, 152
 - hostility to in British law, 378
 - importance of, 169–171
 - importance, compared with authenticity, 341
 - in law, 148–153
 - of letters, 11–12, 144–146, 157–158
 - loss of, 156–169
 - mail and, 145
 - OECD recommendations on, 379
 - Pretty Good Privacy program, 229–230
 - protection for, 144
 - as right, 144
 - Supreme Court decisions on, 189, 319
 - threats to, 153–154
 - Warren and Brandeis on, 147
 - wiretaps and, 207–209 214
- Privacy Act of 1974 (Public Law 93-579), 67, 143, 154, 155, 360
- Private Branch Exchanges (PBX)s, 358–359
 - number of, 368
- Private keys, 68
- Probabilistic cryptography, 343
- Probable words in ciphertext-only attacks, 26
- Product in communications intelligence, 103

- Production of keys, 32–33
- Prohibition era, 148–149, 177–179
- Project Mogul, 92
- Promotion of Commerce On-Line in the Digital Era (PRO-CODE) bill, 247
- Propaganda, 113
- Provocations
 - in electronic intelligence, 349–350
- Public-key cryptography, 38–39, 68, 252, 272, 316, 317
 - in business, 316
 - development of, 68–70, 344
 - NSA opposition to, 70
 - royalties on, 345
 - scale issues and, 316, 317
- Public-Key Infrastructure (PKI), 28, 54, 258
- Public Key Status Report, 227
- Public Law 101-519, 138
- Publication rights, 71–72
- Pueblo*, 97, 349
- Purdue University, 270

- Qu, 254

- RC2 cryptosystem
 - export of, 231
- RC4 cryptosystem, 391
 - export of, 231
- RC6 algorithm, 250, 379
- RCA COMSEC, 376
- RSA cryptographic system
 - development of, 69
 - for digital signatures, 80–81
 - ITAR and, 70
 - NSA opposition to, 72
 - and PGP, 229
 - as possible signature standard, 347
- RSA Data Security company, 72, 252, 253
- Radar installations, vulnerability of, 113
- Radar intelligence (RADINT), 94
- Radar-imaging satellites, 91
- Radford, Charles, II, 198
- Radios, 2
 - detecting station received by, 350
 - frequency-hopping, 44
 - in police work, 134
 - used to deliver products, 337
 - in World War I, 57
- Rafter technique, 94, 350
- Rahman, Omar Abdel, 208, 310, 391
- Ratteni (Nicholas) case, 209
- Rawls, Lee, 369–370
- Reagan, Ronald
 - and CISPEs, 166
 - and drug trafficking, 137, 209
 - and NSDD-145, 74–75
- Real ID Act, 168
- Real-time military intelligence, 113
- Reasonable costs for breaking codes, 26
- Recording Industry Association of America (RIAA), 261
- Records of wiretapping, 194, 207–209, 319
- Reed, Stanley, 158
- Reid, Richard, 310
- Reitinger, Phil, 246
- Reliability in cryptography, 45
- Rendezvous service, 296
- Reno, Janet, 221, 270, 281
- Repetition patterns in cryptography, 20
- Reporters
 - surveillance, 363
- Research cryptanalysis, 102
- Research funding, 71–72
- Retention in communications intelligence, 103
- Revolutionaries, wiretapping of, 195
- Reynolds, Michael, 349
- Rice University, 261
- Right to Privacy Act, 363
- Right, privacy as, 142–144
- Rijndael algorithm, 31, 250, 379
- Rivest, Ron, 69, 72, 229, 250, 253

- Robustness of cryptography, 112
 Rockefeller Commission, 353
 Roman Empire
 identification in, 378
 Roosevelt, Franklin, 180
 Rosenblum, Howard, 344
 Roswell incident, 349
 Rotor machines, 23, 105
 patents for, 58–59
 in Vigenère systems, 23
 for voice, 343
 Routes for messages, 100
 Roving wiretaps, 203, 203, 223, 300
 Rowlett, Frank, 59–60
 Ruckelshaus, William, 164
- S-boxes, 339
 in DES standard, 25
 SAFER algorithm, 379
 SECRET NOFORN classification, 67
 SHA-1 algorithm, 253
 SHA-256 algorithm, 254
 SHA-384 algorithm, 254
 STU-II secure telephones, 340
 STU-III secure telephones, 73–74, 232, 376
 datarate, 343
 delivery of, 345
 digital signal processors in, 376
 funding for, 345
 ignition keys, 376
 Type II, marketing of, 345
 Safire, William, 163
 Sandia National Laboratories, 329
 Sanitization in communications
 intelligence, 103, 352–353
 Satellites, 36
 control of, 350
 footprint of, 351
 for interception, 98–99
 for photographic intelligence, 91–92
 Scale in cryptography, 14–19
 Scherbius, Arthur, 58
 Schmults, Edward, 378
 Schneier, Bruce, 121, 315
 Schnorr, Claus, 81, 347–348
 Schwartz, Herman, 207
Scientific American
 Horst Feistel article in, 344
 Lucifer encryption system in, 344
 Scotland Yard, 134
 Scowcroft, Brent, 227, 376
 Sea of Okhotsk, 351
 Seagulls
 storm detection by, 349
 Search problem, 100
 Search warrants, 149–151, 176, 178–179, 194, 198–199
 Searches vs. wiretapping, 4, 317–318, 318–319
 Searches
 secret, 318–319
 “sneak and peek”, 289
 Search engines, 51
 Sears, John, 163
 Sears Tower, 310
 Secrecy in communications
 intelligence, 103–104
 Secrecy orders for patents, 70, 344
 Secrecy
 success of, 349
 Secret telephone, 354. *See also* Secure voice
 Secretary of State, 360
 Secrets, lifetimes of, 29
 Secure boot, 263
 Secure Data Network System (SDNS), 242
 Secure Digital Music Initiative (SDMI), 260, 261
 Secure hash function, 252
 Secure Public Networks bill, 247
 Secure Socket Layer (SSL) protocol, 32, 43, 52, 56, 259
 Secure Terminal Equipment (STE), 233, 354–355
 Secure communication systems, 46–47
 Secure computing in cryptography, 45
 Secure telephones, 2
 complexity of, 390

- cryptography in, 232–234
- development of, 61–62
- digital, 61–63, 73–74, 340, 343, 345, 354–355
- GSP8191, 390
- limitations of, 110
- STU-II, 340
- STU-III, 73
- TSD 3600, 233–234, 244, 377, 390
- varieties in government use, 376
- Security and Freedom through Encryption (SAFE) bill, 247, 256
- Security clearances
 - in CCEP, 72
 - of escrow agents, 378
 - of NRC panel members, 378
- Security of COMINT, 353
- Security, 11
 - of communications in United States, 117
 - in crime prevention, 127
 - in cryptography, 43–45
 - and intelligence, 117
 - mail and, 145
 - national, *See* National security
- Selection boxes in DES Standard, 25
- Selfridge, Oliver, 356
- Senate Judiciary Committee, 285
- Senate investigation of wiretapping, 200–202
- Sensitive Unclassified Information
 - protection of, 377
- Serpent algorithm, 250, 379
- Service provider, 275
- Session keys, 35, 38
- Sessions, William
 - CISPES investigation comments on, 167
 - on economic espionage, 50
 - on terrorism, 305
- Shamir, Adi, 69, 72, 229, 344–345
- Shannon, Claude, 63 31
- Shapley, Deborah, 70
- SHARK algorithm, 31
- Sheehan, Neil, 197
- Shenker, Morris, 186
- Shielding, 45
- Shift register cryptography, 352
- Shift registers, 23–38
- Shimomura, Tsutomu, 350
- Siemens and Halske T52
 - cryptographic machine, 355
- Sigaba rotor system, 29, 59–61
- Signal processing, 93
- Signaling System 7, 358
- Signaling rules, 26
- Signals intelligence (SIGINT), 93–95
 - 90
 - budget, as fraction of total intelligence budget, 337
 - growth of, 60, 105, 353
 - prospects for, 323
- Signals, interception of, 95–103
- Signatures, digital, 39, 69
- Sigsaly digital telephone, 61–63
- Sigtot system, 45
- Silver cryptosystem, 106
- Julius Silverman et al. v. United States* case, 188
- Simple Mail Transfer Protocol, 270
- Simpson, Jack, 74
- Sinclair, John, 198
- Singapore, surveillance in, 226
- Skipjack algorithm, 9, 25, 235, 237–239, 377, 257
 - Skipjack declassified for protecting email on military networks, 25
- Skype, 56, 111, 259, 298
- Smart cards, 46, 259
- Smith, Jonathan, 263
- Smith, William, 242
- Social Control, mechanisms of, 319, 392
- Social mechanisms, 390
- Socialist Workers Party, 159
 - Damages paid to, 362
 - FBI harassment of, 362
- Societal issues, 330
- Socolar, Milton, 79

- Software Publishers Association
 - deal with NSA, 231, 357
- Solaris, 263
- Solzhenitsyn, Aleksandr, 354
- Sonogram, 354
- Sony Corporation, 263, 274
- Sound Surveillance Underwater System (SOSUS), 92
- South Korea, in cyberattacks, 115, 116
- Soviet Embassy in Washington, D.C., 353
- Soviet Union
 - Cold War, 280
 - communications satellites in, 99
 - defectors from, 391
 - demise of, 118
 - eavesdropping by, 119
 - exports to, 354
 - missile test telemetry of, 350
 - object of US intelligence, 280
 - shootdown of flight KAL 007, 349–350
 - shootdown of U2 spy plane, 349
 - one-time cryptosystems in, 17–19
- Soviet intelligence
 - IBM and, 342
- Spacecraft,
 - for interception, 98–99
 - for photographic intelligence, 91
- Spain, surveillance in, 226
- Spam, 52, 119
- Spare keys, 7, 241
- Specific keys, 13
- Specter, Arlen, 220, 373, 282, 284, 285
- Speed of computations, 27
- Spies, wiretapping of, 195
- Spy satellites, 337
- Spycatcher*, 350
- Spying, 49–50, 89–91
- SQUARE algorithm, 31
- Stages in shift registers, 24
- Standards
 - in cryptography, 53
 - Data Encryption Standard, 24–25
 - Digital Signature Standard, 80–83
 - Escrowed Encryption Standard, 7, 234–241
 - NIST responsibility for, 66, 76–78
- Stanfa, John, 130, 220, 373
- State laws on wiretapping, 212
- Steganography, 259, 338
- Steinbeck, John, 157
- Stipendiary police, 357
- Stoll, Clifford, 114, 358
- Stone, Elliot, 378
- Strategic capability of cryptographic systems, 122
- Stuart, Jeb, 177
- Subpoena
 - for deposit information, 341
- Subscriber keys, 35, 38
- Substitution in cryptography, 19–24
- Subversive activities, 183, 195
- Sugar lobby case, wiretapping abuses in, 196
 - investigation of, 364
- Suite A, 254
- Suite B, 254, 255, 279
 - unclassified algorithms, 254
- Sullivan, William
 - columnist monitored by, 164
 - King discredited by, 160
- Sun Microsystems, 263, 274
- Superposition, 28
- Supporting technologies in cryptography, 45–46
- Supreme Court decisions
 - on bugs, 188–189
 - on identification, 136
 - on privacy, 152, 189, 319, 331
 - on wiretapping, 148–153, 178–179
- Supreme Court justices, wiretapping of, 158, 185
- Surreptitious fingerprinting, 135
- Surveillance,
 - employers and, 278
 - society, 306, 308, 310
 - traffic analysis and, 309, 313
- Surveillance reports

- missing, 368
- Survivability of networks, 354
- Switching systems, 110
- Symmetric cryptosystems, 38
- TSD 3600, 376
 - cost of cryptography in, 390
 - digital signal processors in, 376
 - influence on Clipper chip, 377
 - market for, 377
 - NSA use of, 377
- Taiwan, stolen files routed through, 116
- Talmud, 142
- Tamper resistance, 46
 - of Clipper chip, 377
 - cryptanalysis and, 391
- Tapping. *See* Wiretapping
- Targeting phase of communications intelligence, 97
- Taylor, Anna Diggs, 302
- Technical Working Group (TWG), 79, 81
- Technical intelligence, 93
- Telecommunication systems
 - criminal use of, 369–370
- Telecommunications,
 - impact of, 313–315
 - spying on, 313
- Telegraph system
 - in Civil War, 146
 - copies of telegrams in, 360–361
 - privacy in, 146, 147
 - wiretapping of, 360
- Telemetry intelligence (TELINT), 94, 350
- Telephone Billing Records, 358, 359
- Telephone Frames, as wiretap
 - locations, 131–132
- Telephone records
 - in Foster death, 372
- Telephone scramblers, patent for, 70
- Telephone Security Device, Model 3600, 233–234, 238–239
- Telephone switches, 131–132
- Telephone system 41
 - protection of, 356
- Telephones, 2
 - cordless and cellular, 2, 6, 22, 206, 325
 - court decisions about, 148–153
 - pen registers for, 133, 203
 - secure, *See* Secure telephones
 - wiretapping of, *See* Wiretapping
- Telephony, cryptography in, 232–234
- Teletrack system, 134, 392
- Television
 - used to deliver products, 337
- Tempest protection, 45
 - origin of term, 341
- “Ten Commandments”, 240
- Terrestrial microwave communications, 96
- Terrorism, 374
 - defining threat of, 307–312
 - L.A. 8 and, 167
 - law enforcement and, 139
 - retargeting of intelligence and, 280
 - wiretaps and, 212, 207–209
- Terrorist acts
 - 9/11/2001, 90, 136, 155, 249, 279, 280, 281, 290, 292, 301, 310, 317
 - US jurisdiction over, 138
 - wiretapping targeting of, 211, 224, 389
- Tessera cards, 239, 378. *See also* Fortezza
- Theories of cryptographic security, 339
- Theory of finite fields, 31
- Third Amendment, 144
- Thompson, Larry, 281
- Thompson Ramo Wooldridge (TRW), 350
- Time division multiplexing, 351–352
- Time of computations, 27
- Tina Isa murder
 - electronic surveillance in, 373
- Title III, 192–195, 214, 372
- Tor, The onion router, 272, 273, 274

- and US Department of Defense, 273, 274
- Tracking systems, 134–135
- Traffic analysis, 44, 102, 309, 352, 358
- Traffic keys, 35
- Transactional information, 373
 - CISPES telephone records, 166
 - Clinton, Hillary investigation, 216
 - credit card information, 153
 - pen register, 133, 203
 - trap and trace, 133, 203, 216
- Transactional Records Access Clearinghouse, 311
- Transit traffic, 302
- Transmission Control Protocol, 42
- Transmission security, 44
- Transport layer, 42, 43
- Trap and trace devices, 133, 203, 373
 - expanding use of, 372
- Trap doors, 235, 238, 245
- Traveling in communications, 6
- Travelocity, 274
- Triple-DES cryptosystem, 29, 340
- Truman, Harry
 - NSA approved by, 63
 - wiretapping ordered by, 158, 181, 186, 362
- Trunks for messages, 100
- Trusted Computing Group, 263
- Trusted Computing Platform Alliance, 262
- Trusted Platform Modules, 262
- Trusted Platform Technology, 48
- Trusted transport media, 11–12
- Turing, Alan, 352
- Two-person control, 340
- Two-person key production control, 33
- Twofish algorithm, 250, 379
- Type I and Type II cryptographic equipment, 73, 345
- Type I cryptography
 - keys, escrow of, 377
- Type II cryptography
 - planned exportability of, 377
 - keys, escrow of, 377
- UK-USA treaty, 378
- US Army,
 - Aviation and Missile Command, 116
- US Congress
 - Postal Act of 1792, 145
 - relations with NSA, 346
- US Courts, Administrative Office of, 214, 215, 311
- US Department of Agriculture, 154
- US Department of Commerce, 121, 249
- US Department of Defense, 116, 154
 - NIPRNet (The Department of Defense's Non-Classified IP Router Network), 115
- US Department of Energy
 - opposition to EES, 377
- US Department of Health and Human Services, 154
- US Department of Justice, 154, 280, 281, 283, 310, 270, 372
 - Offices of Professional Responsibility, 282
- US Department of State
 - list of terrorist organizations, 167
 - Early weakness of COMSEC in, 343
- US Federal Aviation Authority, 136
- US Immigration and Naturalization Service, 167, 307, 372
- US Mail (US Postal Service)
 - opening of, 145, 361
 - role in development of US, 148
 - rural delivery, 148
- US lobbying
 - in Britain, 378
- US Marshals Service, 372
- US Office of Management and Budget, 258, 289
- USA PATRIOT Act 140, 168, 319
 - wiretapping and, 280, 281, 283, 284, 319

- Union of Soviet Socialist Republics (USSR). *See* Soviet Union
- Unclassified Sensitive Information, 346
- United States
 - changing world role of, 304
 - cyberwarfare and, 115
 - Constitution, 313
 - data collection by government, 154
 - economic espionage by government, 50
 - Iran and, 107
 - Iraq and, 107
 - privacy in, 144
 - security of communications in, 117
 - Soviet Union and, 107
- United States Commission on National Security. *See* Hart-Rudman report
- United States v. Miller* case, 152, 341
- Universal Declaration of Human Rights, 142
- University of California at Berkeley, 262
- University of California at San Diego, 270
- University of Pennsylvania, 263
- V.fast, 354
- Vanstone, 254
- Venona study, 19, 29
- Valachi, Joseph, 190–192
- Vanstone, 254
- Vapor analysis, 136
- Vela-Hotel satellites, 92, 349
- Venona messages, 338, 353–354
- Verance Corporation, 261
- Verheul, Eric, 252
- Video Privacy Protection Act, 153
- Video cameras, 135
- Video recordings, 3
- Video rental records
 - privacy of, 361
- Vietnam War
 - protests against, 161–162, 165, 320
 - wiretapping abuses during, 196–198
- Vigenère cryptosystem, 338–339
- Vigenère, Blaise de, encryption scheme by, 21–23
- Vinson, Fred, 158
- Viruses and worms (in computers), 114, 118, 119, 356
 - origin of, 356
- Vocoders, 61–62
- Voice scramblers, 61, 343, 354
- Voice-encryption systems, 233
- Voice over Internet Protocol (VoIP), 55, 56, 111, 259
 - and wiretapping, 295–299
- Volkswagen, 341
- Wagner, David, 262
- Wang, Xianyun, 253
- Ward, Daniel, 193
- Ware, Willis, 376, 378
- Warrants. *See* Search warrants
- Warren, Samuel, 147
- Watchers, 350
- Watergate affair, 199–200, 337
 - electronic surveillance in, 337
- Watermarks, 49, 259, 261
- Weblogs, 51
- Websites,
 - break-ins, 118
- Webster, William, 168
- Weingarten, Frederick, 71
- Western Union, 146
- White House. *See* US Office of Management and Budget
- Whitworth, Jerry, 34
- Wirephotos, 134
- Wiretapping, 203, 319, 358, 371
 - admissibility of, 372
 - authority, expansion of, 373, 375
 - British, 374–375
 - vs. bugs, 188–189
 - CALEA and, 294–301
 - California and, 212
 - in civil rights movement, 184
 - constraints on, 216–218
 - convictions from, 212–216
 - costs of, 218

- court decisions about, 148–153, 178–179
 court orders for, 194, 198–199
 data on, 207–208, 319
 defense use of, 368, 372
 dependence on, 7
 disapproval of, 368
 for domestic national security, 195–199
 drug cases, use in, 369–370
 and Electronic Communications Privacy Act, 203
 emergency orders for, 372
 as entrapment, 208
 and encryption, 227, 244, 319
 espionage cases, use in, 369–370
 European Union and, 375
 evidence vs. intelligence from, 179–188
 expansion of, 373
 and Foreign Intelligence Surveillance Act, 202–203
 incriminating conversations overheard in, 368
 international support for, 224–226
 Internet, 269
 in kidnapping cases, 211, 369–370, 391
 in law enforcement, 128–131, 194
 legalization of, 192–195
 limits on, 193–195
 minimization of, 372
 in nineteenth century, 177
 operation of, 131–133
 and organized crime, 189–192, 194, 209, 369–370
 in police textbooks, 392
 political purposes in, 184–185, 195–198
 reporting of, 372
 roving, 203, 203, 223, 300
 vs. searches, 4, 317–318
 Senate investigation of, 200–202
 state laws on, 212
 targeting of, 209–211
 techniques of, 358
 terrorism cases, use in, 369–370
 Title III, 214
 types of, 358
 USA PATRIOT Act and, 281, 283, 284, 285
 usefulness in court decisions, 207–209
 value of, 206
 VoIP and, 295–299
 in Watergate, 199–200
Wiretap Report, 212, 215, 311, 370, 370, 384
 anomalous figures in, 371
 convictions in, 368
 multiple crimes in, 368
 Women's liberation movement, 162
 Woolsey, James, 255
 Workfactors in cryptography, 27–28
 World Trade Center bombing, 310, 328, 359
 World War I, 57
 World War II, 61–62
 cryptosystems, 352
 World Wide Web, 51, 89, 264
 English language becoming less dominant, 266
 Worms, 118, 119
 Wright, Peter, 106, 350
 Wright, Sydney Fowler, 357–358
 Writs of assistance, 176
 X-ray machines, 136
 Y2K, 289
 Yahoo, 264
 Yin, Lisa Yiqun, 253
 Yom Kippur War, 350
 Yousef, Razmi, 208
 Yu, Hongbo, 253
 Zero-Knowledge Systems, 262, 272
 Zfone, 56
 Zimmermann, Philip, 229–230
 Zombies, 119